NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CYBERCIEGE SCENARIO ILLUSTRATING PKI INTEROPERABILITY ISSUES THROUGH E-MAIL COMMUNICATIONS IN A CORPORATE ENVIRONMENT

by

Ng Teng Teng

December 2011

Thesis Co-Advisors:	J. D. Fulp Mike Thompson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE A CyberCIEGE Scenario Illustrating PKI Interoperability Issues through E-mail Communications in a Corporate Environment	**5. FUNDING NUMBERS**
6. AUTHOR Ng Teng Teng	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. I.R.B. Protocol number __N.A.__

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

To help educate computer/network users and administrators on the complexities and potential implementation pitfalls of PKI, the work outlined in this thesis extended the CyberCIEGE computer security simulation game with additional PKI-related functionality. The research developed a scenario definition file for the CyberCIEGE game engine that supports a new game scenario that illustrates PKI concepts (e.g., cross-certification, certificate path processing and certificate revocation), configuration choices, and the security implications thereof. The game engine was enhanced to realistically model the parameters of an actual X.509 digital certificate. Test cases designed for this game extension verified that the scenario reasonably portrayed realistic PKI deployment issues and provided feedback consistent with real-world PKI implementations.

14. SUBJECT TERMS Public Key Infrastructure (PKI), X.509 Certificate, Certificate Revocation, Certificate Path Processing, CyberCIEGE, Computer security education	**15. NUMBER OF PAGES** 90
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

A CYBERCIEGE SCENARIO ILLUSTRATING PKI INTEROPERABILITY ISSUES THROUGH E-MAIL COMMUNICATIONS IN A CORPORATE ENVIRONMENT

Ng Teng Teng
Civilian, Ministry of Defense, Singapore
B.S., (Hons), National University of Singapore, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Ng Teng Teng

Approved by: J.D. Fulp
Thesis Co-Advisor

Mike Thompson
Thesis Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To help educate computer/network users and administrators on the complexities and potential implementation pitfalls of PKI, the work outlined in this thesis extended the CyberCIEGE computer security simulation game with additional PKI-related functionality. The research developed a scenario definition file for the CyberCIEGE game engine that supports a new game scenario that illustrates PKI concepts (e.g., cross-certification, certificate path processing and certificate revocation), configuration choices, and the security implications thereof. The game engine was enhanced to realistically model the parameters of an actual X.509 digital certificate. Test cases designed for this game extension verified that the scenario reasonably portrayed realistic PKI deployment issues and provided feedback consistent with real-world PKI implementations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

FBCA	Federal Bridge Certification Authority
CA	Certification Authority
CRL	Certificate Revocation List
CISO	Chief Information Security Officer
IETF	Internet Engineering Task Force
LRA	Local Registration Authority
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
TLS	Transport Layer Security

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Many individuals have provided me with invaluable advice and positive encouragement during the development of this thesis. I would like to take this opportunity to extend my heartfelt gratitude to them.

I wish to thank my family and loved ones for their understanding and moral support.

I would like to express my sincere appreciation to J.D. Fulp and Mike Thompson, my advisory team for this thesis work. Thank you for all your patience, guidance, time and constructive feedback.

Finally, I would like to thank my sponsor, the Defence Science and Technology Agency (DSTA), for offering me the scholarship to enroll in this enriching master’s course at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

The purpose of this thesis is to develop educational information security scenarios that highlight the most prominent issues related to proper implementation of Public Key Infrastructure (PKI) solutions for incorporation into the CyberCIEGE game engine. CyberCIEGE, jointly created by the Naval Postgraduate School’s Center for Information Systems Security Studies and Research and Rivermind, Inc. (Irvine & Thompson, 2010), is an interactive video game that is used to enhance computer security education through a series of scenarios that highlight Information Assurance concepts and training objectives.

In pursuit of the above primary thesis objective, this research sought to answer the following subsidiary questions:

1. What is the target student/player profile (i.e., level of difficulty/detail) of the CyberCIEGE game?
2. What are the pertinent/prominent policy and operational variables surrounding the implementation of PKI in the real world?
3. Can actual digital certificates (e.g., X.509) used in real-world PKI be integrated into CyberCIEGE? If not, what are the most apropos elements of an “actual certificate” that should be included in the game’s abstraction of a certificate?
4. Of the identified pertinent (PKI) variables, which are the best candidates for inclusion into the CyberCIEGE game environment; as predicated by any limitations of the game, or educational bounds regarding the target student/player profile?
5. What is an ideal “story board” (game scenario) that would best serve to focus a player’s attention on those identified best PKI variables?

B. RELATED WORK

The CyberCIEGE game engine was recently expanded to include PKI features, including certification authorities, selection of installed roots and cross certification (Irvine & Thompson, 2010). The game engine modifications include modeling of chains of trust and potential risks with cross certification schemes. The enhancements proposed in this thesis, which are focused on a typical corporate environment, augments the current PKI features of the game in order to further illustrate PKI security and interoperability issues involved with e-mail communications.

C. THESIS SCOPE AND LAYOUT

This thesis research encompasses three main areas:

1. Study of Current State of PKI Implementations in the Real World

The first phase of the study entailed research on the current state of PKI implementations and applications in the real world. Pertinent variables that determine different types of PKI configurations are identified, then these variables are analyzed against organizational goals (e.g., business cost and benefits) to determine the optimum PKI configuration.

2. Development of a Scenario to Represent the Identified PKI Application

A CyberCIEGE scenario was developed to allow players to understand the different security implications of varied PKI configurations based on an identified PKI application from the initial study. The existing CyberCIEGE game engine PKI features were analyzed and game engine extensions were proposed to support the scenario.

3. Enhancement of CyberCIEGE User Interface to Represent Actual X.509 Certificates

Prior to this thesis, CyberCIEGE's representation of a PKI certificate was limited to brief descriptions of the certificate's subject and its issuing Certification Authority. This thesis enhanced certificate representation by adding additional, select, X.509 certificate attributes. The additional attributes were chosen in order to give players a better understanding of how the different parameters in a certificate affect the security of PKI operations.

This thesis is presented in the following chapters:

- Chapter I–Introduction. This chapter defines the thesis statement and scope. It lists some of the previous work related to this thesis and also provides an overview how the report is being structured.
- Chapter II–Background. This chapter describes the CyberCIEGE project and how it can be used as an effective educational tool to relate PKI operational considerations. It further presents the key concepts of PKI and provides an overview of PKI in practice, before identifying the specific PKI elements that will be modeled in the CyberCIEGE scenario.
- Chapter III–Scenario Strategy. This chapter discusses the educational goals which the scenario aims to achieve and establishes the framework for the scenario development.
- Chapter IV–Scenario Description. This chapter describes the simulated gaming environment that is being modeled by the scenario definition. It includes the player briefings, objectives, assets to be protected and e-mail policies that are depicted in the scenario.
- Chapter V–Scenario Testing. This chapter covers the test objectives and strategies to verify the correctness of the certificate attack scenario. It includes the scope, expected results and actual results of the test case.

- Chapter VI–Conclusion. This chapter summarizes the research and work done for this thesis and proposes additional areas for future research.

II. BACKGROUND

A. COMPUTER SECURITY AWARENESS AND TRAINING

With the advancement of Information Technology, computers have become an all-essential asset for many organizations, hosting various applications ranging from mission-critical weapon systems to peacetime administrative portals. We have seen a shift in management's emphasis from merely deploying functional IT implementations, to increased awareness of and attention to computer security threats and defenses. Despite this increased awareness from management, user behavior has not changed significantly. Users will often opt for the easiest and most convenient means of achieving their work goals. User security typically extends only to what security administrators have configured into their computers, or perhaps specific security policy mandates that are drilled into daily operations. Without understanding the rationale behind the security measures that are in place, users are more likely to take the paths of least (security) resistance. Education and training in computer security is often mundane and boring for both users and administrators (Irvine & Thompson, 2003).

Computer security is constantly evolving and requires security practitioners to be up-to-date and well-informed. The traditional textbook style of security education and training can no longer suffice to edify users on complex security policies and technologies. The challenge remains to find an IT security education tool that is both effective, adaptive, and more interesting than plain text descriptions of complex security technologies and interdependencies.

B. CYBERCIEGE AS AN EDUCATIONAL TOOL

CyberCIEGE, an interactive simulation game that is used to enhance information assurance education and training through constructive resource management techniques, is a natural choice for computer security educational tool.

In the CyberCIEGE interactive environment, players are guided through a series of scenarios that highlight various cyber security education and training objectives. In each scenario, players assume the role of the IT manager who must keep the IT infrastructure running in support of various enterprise goals, while making tradeoffs and prioritization decisions as they are challenged to maintain a balance between budget, productivity and security. The consequences of these choices are reflected in the success of either the enterprise or of external adversaries, which will determine if the player achieves his game objectives (Irvine & Thompson, 2010; Allen, Irvine, & Thompson, 2005).

The game also contains encyclopedia entries and edifying movies that explain and illustrate how certain security mechanisms work. The rich features in CyberCIEGE provide an ideal platform for developing new coursework for training and education in information assurance, including demonstrating the concepts of identification, authentication, provenance, and access control in inter-/intra-corporate communications. The simulation environment allows players to understand the bigger picture implications of IT/security decisions that have to be made in the real world; a perspective which would otherwise be challenging to experience in the real world given limited resources and the real fear of making errors affecting operational systems.

This thesis will look into providing the game with a new scenario, and potentially extending the game engine, to more realistically model the actual parameters of PKI configuration and to enhance player understanding of PKI choices, trade-offs, and concepts. This will complement traditional seminar-style education to provide a comprehensive learning experience to the players. The scenario will also provide a taxonomy of real-world PKI implementations for future analysis and reference.

C. KEY CONCEPTS OF PKI

A Public Key Infrastructure (PKI) is the basis of a pervasive[1] security infrastructure whose services are implemented and delivered using public-key concepts and technique (Adams & Lloyd, 2003). It consists of a set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates ("Public Key Infrastructure," 2011). The following section explores the fundamental PKI concepts as well as public-key certificates and certificate revocation schemes in greater detail.

1. Primary PKI Elements

A fully functional PKI is composed of a large set of components and services.

a. Certification Authority (CA)

A Certification Authority is a trusted entity whose primary role is to sign and publish a certificate binding a public key pair to a user identity. The CA is a critical component in large-scale PKIs, but may not be present in small-scale PKIs as they might rely on external CAs to establish the trust hierarchy, which will be discussed in Section 3.

b. Registration Authority (RA)

Although the registration function can be implemented within the CA component, it is often delegated to a separate component called the Registration Authority. The RA is a trusted entity that is responsible for identification and authentication of certificate subjects, but does not issue certificates or CRLs (Federal PKI Policy Authority, 2007). Activities overseen by the RA may include establishing and confirming the identity of an individual, enrollment and registration, credential issuance and credential revocation.

[1] An infrastructure may be considered a *pervasive substrate*, which is a foundation or underpinning for large environment such as a corporate organization.

The RA may also delegate functional roles and duties to a Local Registration Authority (LRA), which is essentially a smaller-scale RA, to enhance scalability and decrease operational costs.

c. Certificate Repository

A certificate repository is a collection of all the root certificates located in an end user's workstation, which is used to establish the roots of webs of trust.

d. Certificate Revocation

Every certificate has an expiry date, but in the event that the certificate has been compromised (e.g., the laptop that contains the private key associated with a certificate has been stolen) before its expiration date, proper certificate management requires that there be some means of revoking the certificate so that any relying party will know that it is no longer valid and should not trust any transaction dependent upon it.

e. Key Backup and Recovery, Key Update and Key History

Real-world PKI users may lose their private keys (e.g., lose the smart card storing the PKI keys) within the certificate lifetime. Key backup (escrow) and recovery mechanisms allow such keys to be restored to prevent inaccessibility of data protected by the lost keys. Key updates, on the other hand, generate new keys to replace the existing ones, typically when a certificate expires, is revoked, or when there is a need to change the key lengths with respect to the encryption algorithms.

Key histories must be managed to keep track of the users' old keys and current keys in order to use the correct decryption key to decrypt the required data.

f. Client Software

PKI is essentially a client-server architecture whose server entities provide a collection of services to the end users (certificate owners and certificate users), such as the following (Adams & Lloyd, 2003):

- The CA provides certification services.
- The RAs implement end-entity registration functions.
- The repository holds certificates and revocation information.
- The backup and recovery server manages private keys.

Client software, on the other hand, implements the required client end of the PKI services on the end-user's local platform, such as the following:

- requests certification services;
- initializes registration process;
- asks for certificates and process relevant revocation information; and
- understands key histories and requests for key updates/recovery when necessary.

2. Certificate Structure

The Internet Engineering Task Force (IETF) introduced the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile (Housley, Polk, Ford, & Solo, 2002), which describes the generic structure of the X.509 certificate. Figure 1 shows the current Version 3 X.509 certificate structure, where some of the fields are further defined below:

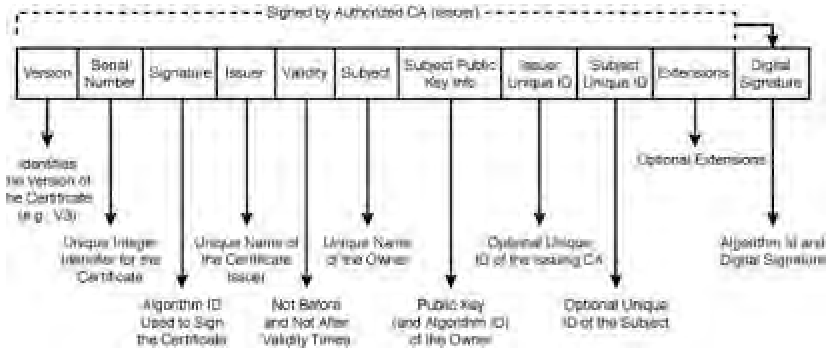

Signed by Authorized CA (issuer)
Version
Serial Number
Signature
Issuer
Validity
Subject
Subject Public Key Info
Issuer Unique ID
Subject Unique ID
Extensions
Digital Signature
Identifies the Version of the Certificate (e.g. V3)
Unique Integer Identifier for the Certificate
Algorithm ID Used to Sign the Certificate
Unique Name of the Certificate Issuer
Not Before and Not After Validity Times
Unique Name of the Owner
Public Key (and Algorithm ID) of the Owner
Optional Unique ID of the Issuing CA
Optional Unique ID of the Subject
Optional Extensions
Algorithm Id and Digital Signature

Figure 1. Version 3 X.509 certificate structure (From Adams & Lloyd, 2003)

- *Signature* contains the algorithm identifier for the algorithm used by the CA to sign the certificate.
- *Issuer* identifies the entity which has signed and issued the certificate. It must always be present.
- *Validity* indicates the period during which the certificate is considered valid, unless it has been revoked.

Extensions defined for X.509 v3 certificates are optional methods that help to associate additional attributes with users or public keys and for managing a certification hierarchy. An extension may be marked critical, which means that it must be recognized and processed "successfully" (its semantics satisfy the contingent security requirement that the extension addresses), otherwise the certificate will be rejected. A non-critical extension may be ignored if it is not recognized.

The standard and private extensions that are available in X.509 v3 certificates are: Authority Key Identifier, Subject Key Identifier, Key Usage, Extended Key Usage, CRL Distribution Point, Private Key Usage, Certificate Policies, Policy Mappings, Subject Alternative Name, Issuer Alternative Name, Subject Directory Attributes, Basic Constrains, Name Constraints, Policy Constraints, Inhibit Any Policy and Freshest CRL Pointer.

Some of the key extensions that have been deemed relevant to embellish the CyberCIEGE scenario in order to meet the learning objectives which we hope to impart as part of this research are elaborated below:

- *Key Usage* is a bit string used to identify the function (e.g., digital signature, data encipherment, certificate signing) of the public key contained in the certificate.

- *Extended Key Usage* is a sequence of OIDs[2] that indicates one or more applications for which the certified public key may be used, in addition to the functions specified under *Key Usage* field. Some of these applications include: Transport Layer Security (TLS) web server/client authentication, code signing, e-mail protection, time stamping and Online Certificate Status Protocol (OCSP) signing (Housley et al., 2002). (OCSP will be further discussed in section 4.)
- *CRL Distribution Point* states the location where the PKI client software can refer to for the revocation information associated with the certificate in question.
- *Certificate Policies* contains a sequence of OIDs and optional qualifiers that indicate requirements and restrictions associated with the intended use of the end-entity certificates issued by a given CA under a specific policy. These policy requirements and restrictions will—among other things—establish acceptable policy regarding certification path validation. For example; policy may limit path length from the end-entity certificate to the issuing/root certificate (Housley et al., 2002).

3. Trust Models

In the context of PKI, the notion of trust is often associated with public keys. In particular, an end entity trusts a Certification Authority (CA) when the end entity assumes that the CA will establish and protect the veracity of the binding between the identity of a subject and the public key associated with the subject (Fulp, 2011).

a. Strict Hierarchy of CAs

The trusted CA would form the root of the certification hierarchy, or “trust anchor,” for the entire domain of PKI entities in that hierarchy, as shown in Figure 2.

[2] OID stands for ObjectIdentifier, which is a unique representation for a given object (Adams & Lloyd, 2003).

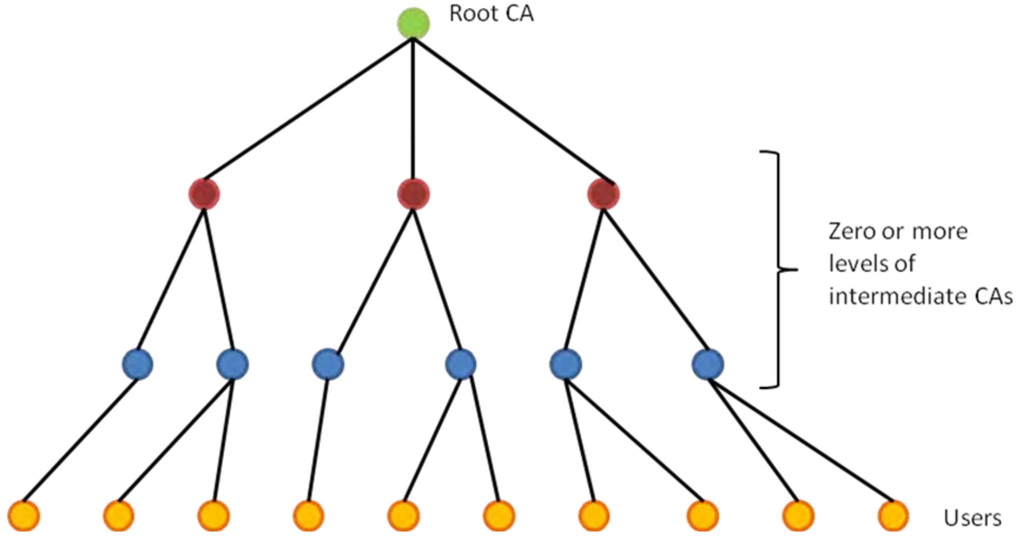


Figure 2. Strict hierarchy of CAs

The root CA will issue and publish a self-signed certificate, which will be used as a basis of trust for all the entities in the hierarchy. The root CA will also sign and issue certificates to the intermediate CAs at the next level; the intermediate CAs will in turn sign and issue certificates to the certificate owners at the lower level.

b. Distributed Trust Architecture and Cross-Certification

A distributed trust architecture is formed by interconnecting independent strict hierarchies of CAs, as illustrated in Figure 3. This model is more reflective of the real world, where each disparate organization implements her own PKI and these PKIs do not necessarily emanate from a common root CA, yet need to establish secure communications with one another nonetheless.

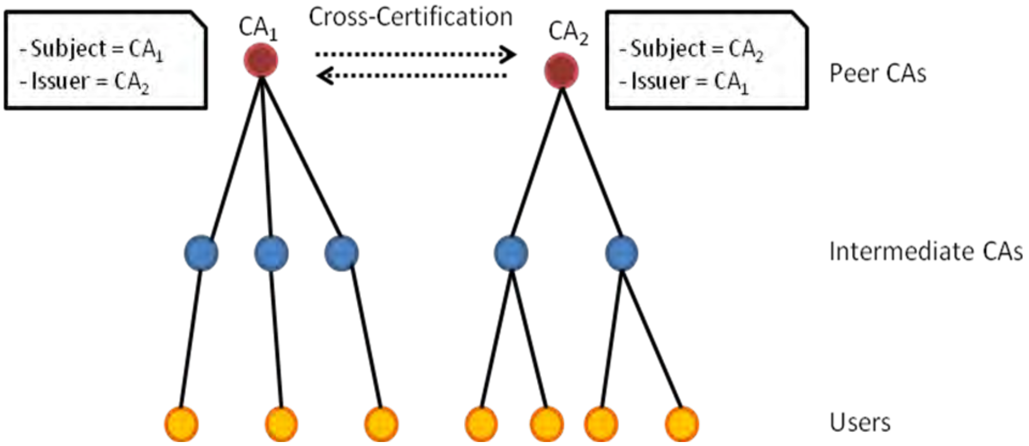


Figure 3. Distributed trust architecture model

Cross-certification is the process wherein one CA attests to the authenticity of another CA's public key. This is cryptographically affected via the attesting CA "signing" (encrypting with its private key) the hash of the other CA's credential information with that other CA's public key. When this process is reciprocated there is a bi-directional expression of trust between the two separate PKI hierarchies. This cross-certification enables trust to be extended between users from the two related CAs. In Figure 3, CA_1 is aware that CA_2 is authorized to issue certificates in CA_2's domain and hence will be able to validate entities in CA_2's domain, hence establishing interoperability.

c. Certificate Path Processing

Certificate path processing is the process of establishing a chain of trust all the way up to the root of the hierarchy, or the trust anchor, such that the certificate can be validated against a recognized root CA in the certificate repository. The target certificate is trusted only if every certificate in the path is examined to be trustworthy. In order to "walk the chain," the relying party's client software would have to download and validate the certificate of every entity in the path for which it did not already have locally available. Alternatively, the target could send some or all certificates in its ancestral chain to the relying party along with the signed message (Fulp, 2011).

4. Certificate Revocation

As discussed earlier, part of the validation process performed by the PKI client software includes checking the revocation status of the target certificate. The software would have to either retrieve the revocation information directly from a CRL distribution point, or to query the revocation information from a trusted third party via the Online Certificate Status Protocol (OCSP).

CRLs are basically data structures that contain a list of revoked certificates, signed and maintained by the same CA that issued those certificates. The list has to be updated and published regularly so that compromised certificates would be rightfully ignored. The generic structure of the CRL is represented in Figure 4 (Adams & Lloyd, 2003).

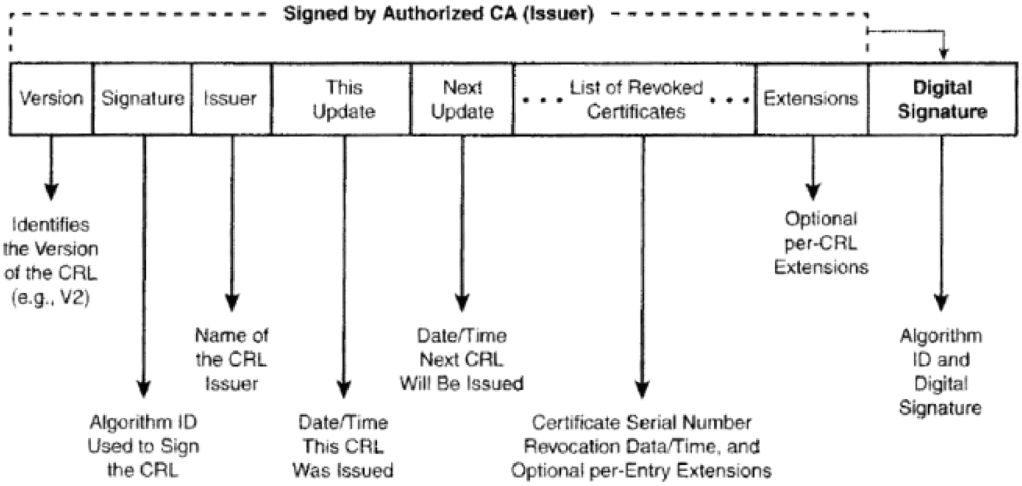

Signed by Authorized CA (Issuer)
Version
Signature
Issuer
This Update
Next Update
. . . List of Revoked Certificates . . .
Extensions
Digital Signature
Identifies the Version of the CRL (e.g., V2)
Optional per-CRL Extensions
Name of the CRL Issuer
Date/Time Next CRL Will Be Issued
Algorithm ID and Digital Signature
Algorithm ID Used to Sign the CRL
Date/Time This CRL Was Issued
Certificate Serial Number Revocation Data/Time, and Optional per-Entry Extensions

Figure 4. CRL structure (From Adams & Lloyd, 2003)

OCSP is a simple request-response protocol that allows a relying party to query the revocation status of a given certificate from a trusted entity known as an OCSP responder. It requires the relying party and the responder to be online. The response will include the certificate status, certificate validity, and time and reason of revocation if the certificate has been revoked. In general, OCSP can provide more real-time and up-to-date revocation information as compared to an offline CRL distribution point.

5. Protection of Private Keys

One of the main purposes of the certificate is to prove possession of private key without revealing information about it. It is thus necessary to protect the private key from compromise or loss (22nd Open Grid Forum, 2008). If the private key is lost, not only must a new certificate be created and redistributed, trust and procedures may have to be reestablished as well. In the case of a compromise, the attacker can now use the private key maliciously. Even a full-fledged PKI can no longer guarantee the integrity of the subscriber and support non-repudiation.

Private key management is a non-trivial task. Some important considerations to ensure a secure key life-cycle management include the location of the key-pair generation, the need to generate multiple key-pairs per end entity to support distinct applications, and the secure storage of private keys (e.g., in smart cards). The distribution of private keys often has to be augmented with administrative procedures and dedicated distribution channels to ensure that the private key could not possibly have been accessed by anyone other than its rightful owner and any authorized escrow (backup) authority.

6. Assurance

The success of PKI is based upon the trust that an end entity places on a Certification Authority. This translates to having confidence in the robustness of the processes and procedures that a CA has in place for end-entity registration as well as the security controls it has in place to protect its own signing private key. The problem is that certificates from a trusted CA may be accepted unconditionally, yet their integrity cannot be easily verified. A breach in the CA will result in fraudulent certificates being issued and PKI relying parties basing their trust on these fraudulent certificates. Further, failure to verify that a CA issuer is itself a recognized/respected/trusted CA sets up the PKI user community for “bogus” certificates being used to secure various electronic transactions (Hofman, 2011; Bright, 2011).

Time-stamping is another critical element in the support for non-repudiation. There must be an authoritative time source for the entire domain of PKI entities, in order to validate that the document contents were not tampered with subsequent to the application of the digital signature.

D. PUBLIC KEY INFRASTRUCTURE (PKI) IN PRACTICE

The ubiquity of computing has led to more applications and services being developed and deployed online to reach out to the mass consumer market. Some of these applications involve sensitive financial data and personal identifiable information, which has called for the need for strongly authenticated and trusted transactions. As commercial organizations become more conscious of their cyber security needs, they increasingly recognize the value of PKI technology to attain their identity management and data security goals. We also see continued PKI growth within the Federal government, spurred by Federal agencies needing strongly authenticated, trusted transactions: a) within the Federal agency; b) between itself and other Federal agencies; and c) with external entities (e.g., business partners, state and local governments, constituents) (ICAMSC, 2010).

Currently, we see the integration of PKI into the following applications:

- E-mail clients (encryption and/or authentication of e-mails)
- Root stores of major internet browser and operating systems
- Word processors and readers (encryption and/or authentication of documents)
- Web and thick client applications (user authentication via Smart Cards)
- Secure communication protocols (bootstrapping of public key methods in the initial protocol setup)
- Code signing

1. PKI Implementation Considerations

PKI technology is mature, as evidenced by the emergence of identity management and security standards that increasingly utilize PKI (ICAMSC, 2010). Nevertheless, we must be aware of the issues and decisions involved in the deployment and operation of a PKI.

a. Trust Models: Hierarchical versus Distributed

The Federal PKI follows a distributed trust model, where the Federal Bridge CA (FBCA) maintains bilateral cross-certification with multiple federal agencies and commercial service providers, such as the Department of Defense (DoD), United States Postal Service (USPS), VeriSign, etc. (ICAMSC, 2010). This model is more flexible compared to the hierarchical model as it allows CAs to be dispensed with minimal disruption to the other interconnected CA domains. In the event that the Federal Bridge CA goes down (e.g., compromise of the CA's signing private key), other Bridge CAs that were cross-certified with it may still validate the entities that were certified by the FBCA.

b. In-Sourcing versus Out-Sourcing

Some of the common factors that affect the decision of whether to in-source or out-source PKI services include economic considerations and the source of trust. For example, a military organization may choose to maintain total control over their PKI, as they do not wish to depend on a third-party service provider to manage the keys that are used to protect their classified data. On the other hand, a smaller commercial enterprise may opt for out-sourcing (e.g., pay VeriSign to issue a certificate bound to the company) due to economic and resource constraints.

c. Certificate Policies

Certificate policies have to be properly defined as they list the requirements and restrictions associated with the intended use of the certificates issued under the policy. Specifically, formal agreements need to be established between enterprise domains that want to communicate under one or more inter-domain policies (Adams & Lloyd, 2003), to facilitate interoperability. This means that the public key certificates have to be populated with the *Certificate Policies* extension to support this requirement and the client software has to be capable of interpreting these business controls during certificate path processing.

d. Online versus Offline Operations

As discussed earlier, using OCSP requires end-users to be online in order to perform the certificate revocation checks. However, this may not be suitable for certain operations, e.g., when user has to validate a certificate in an offline operation. In this case, CRLs and the necessary certificate chains may be cached to enable offline certificate validation. It is also important to note that the security of offline operations is often reduced as the CRLs are not up-do-date and time-stamping service is no longer available.

e. Hardware Requirements

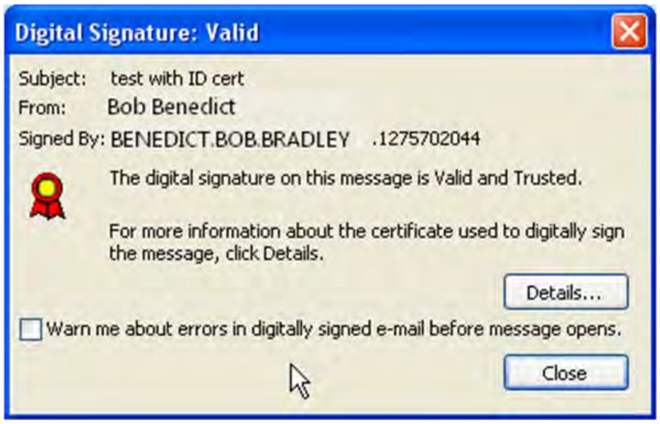
Pure-bred software PKI implementations may be susceptible to Trojan horses and network attacks and hence should be complemented with hardware component, such as the Smart Card, to store private keys and other sensitive information. The middleware that sits between the hardware device (e.g., the Smart Card reader) and the PKI client software must also be capable of extracting the relevant information from the Smart Card when required. For example, during a TLS web client authentication, when the user is prompted to login using his Smart Card, the middleware should only show certificates with *Key Usage* extension of type *digitalSignature* and obscure those of type *dataEncipherment*. When multiple certificates are available, we observe that the decision still lies with the user to determine the correct certificate to be used. This is a typical example showing the tradeoff between interoperability and security.

2. End-User Behavior

Consider an e-mail scenario in which PKI is integrated into the e-mail client using Secure Multipurpose Internet Mail Extensions (S/MIME). When Alice receives a signed e-mail from Bob, her S/MIME application would examine the certificate that comes with the e-mail. Alice’s S/MIME application would first verify if Bob’s certificate resides in the trusted end-entity certificate store. If not, it will try to locate the CA certificate that was used to sign Bob’s certificate in its set of root certificates or the trusted CA certificate store (ones that have been imported by Alice previously). If the CA certificate does not exist, the S/MIME application would then perform certificate path processing to construct the entire certificate chain that leads up to Bob’s root CA and validate the correctness of the signature, check validity period, check for revocation, and check other critical fields in the certificate (e.g., key usage).

If the entire certificate chain cannot be obtained, or any of the certificates fail to validate, the S/MIME software would pop up a dialog box that says “The digital signature cannot be verified. Do you want to proceed?” Alice, and the majority of the users, would simply click OK without understanding the implication of that decision. Bob’s certificate is now added to the trusted end-entity certificate store and the next time Bob’s message arrives, it would naturally be verifiable.

Now, suppose Bob has three different keys; one for data encryption, one for digital signing and one for identification; and he chooses to sign an e-mail to Alice using his identity key. Alice’s e-mail client should flag the e-mail as suspicious and pop up a dialog box to warn Bob. Interestingly, we observed that different e-mail clients handle anomalies in certificates differently, as illustrated in Figures 5 and 6. Microsoft Outlook 2007 did not detect the anomaly and stated that the digital signature is valid and trusted, while Mozilla Thunderbird gives a warning noting that the sender’s certificate did not include an e-mail address, since Bob’s e-mail address would only be associated with his digital signature key, but not his identity key.



Digital Signature: Valid

Subject: test with ID cert

From: Bob Benedict

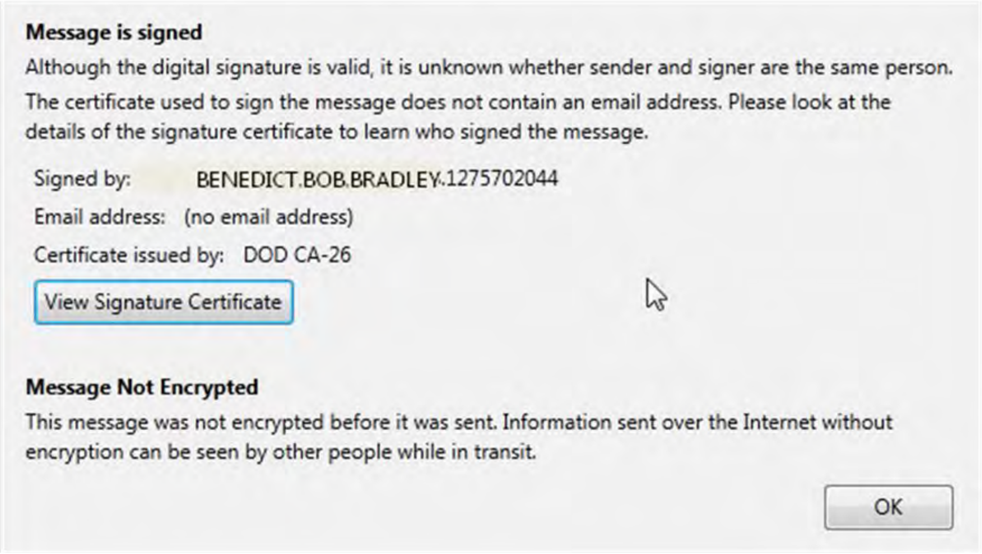
Signed By: BENEDICT.BOB.BRADLEY .1275702044

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

□ Warn me about errors in digitally signed e-mail before message opens.

Figure 5. S/Mime response on Microsoft Outlook



Message is signed

Although the digital signature is valid, it is unknown whether sender and signer are the same person. The certificate used to sign the message does not contain an email address. Please look at the details of the signature certificate to learn who signed the message.

Signed by: BENEDICT.BOB.BRADLEY.1275702044

Email address: (no email address)

Certificate issued by: DOD CA-26

Message Not Encrypted

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

Figure 6. S/Mime response on Mozilla Thunderbird

With respect to handling of different S/MIME responses, user training and awareness will always be helpful to ensure users understand the ramifications of their decisions and potential risks therein. If users are trained to recognize the consequence of their decisions, the security afforded by PKI services can be improved. This will be one of the factors that influence the selection of components to be modeled into CyberCIEGE to allow players to go through the scenario and understand the different security implications of their actions.

E. SELECTION OF PKI ELEMENTS TO BE MODELED INTO CYBERCIEGE

1. Selection Criteria

As presented in the previous section, there are many variables that define different types of PKI configurations. We have discussed some of the business drivers and modes of operations that influence the choice of these variables and the corresponding technical requirements that have to be in place to support the identified PKI configuration.

The next question is to consider which of these variables should be modeled into CyberCIEGE to fully enhance the learning experience of the players. Based on the existing PKI implementations in the real world and the various implementation considerations, we have drawn up the key learning objectives which the players will benefit from in this PKI study, which will eventually translate to the exact elements modeled into CyberCIEGE.

- Understand the real-world deployment issues and decisions, especially relevant when players are posted back to their organization to work in the cyber security field.
- Note the subtleties in some of the PKI configurations and how attackers could make use of these to overcome the security controls, even for a full-fledged large scale PKI.
- Recognize the implication of unwitting security decisions (e.g., clicking OK without even reading or understanding the warning text that may cause an “untrusted” certificate to be permanently placed in a “trusted” store).
- Relate to the course material of CS3690 Network Security, on the topic of *Authentication*.

Table 1 summarizes the list of PKI elements to be modeled into CyberCIEGE for this study, as well as an explanation regarding why and how they are being modeled.

Table 1. List of PKI elements to be modeled into CyberCIEGE

PKI Element	**Why and How is it being modeled?**
Cross-certification	With the increase in the use of a distributed trust model, it would be useful to illustrate how secure communications between different PKI hierarchies is enabled through the use of cross-certification. Players will be able to observe how different organizations with different CAs are able to exchange e-mails through the cross-certification mechanism.
Certificate path processing	One of the key benefits of PKI includes strong authentication, which translates to trusting the validation of the entire certificate chain. Players will be able to observe the certificate chain constructed by the e-mail client and personally validate the correctness of the individual fields of the certificate.
Certificate revocation	Part of the validation process described above includes checking the revocation status of the target certificate. Players will be able to observe how malicious attackers send spoofed e-mails through a compromised laptop containing the user certificate and how CRL implementation can overcome this vulnerability.
X.509 certificate structure	Certificates are the basis of PKI transactions. It is noteworthy to delve into some of the fields of the certificate structure in order to better visualize and comprehend the processes involved in validation, e.g., in certificate path processing and certificate revocation.
Certificate extensions	Certain extensions in the X.509 certificate are critical and must be processed and understood as part of the validation process. These include *Key Usage*, *Extended Key Usage* and *CRL Distribution Point*, which will be modeled as part of the X.509 certificate structure. In order to avoid confronting players with the administrative minutia of actual OIDs used to indicate the applications for which the certificate may be used, it was considered more useful to model these as textual descriptions in the Certificate Purpose tab (further described in Chapter III).
Certificate policies	Certificate policies need to be defined in order to promote interoperability between different organizations. In order to enhance the learning experience of players, it would be more meaningful to model these as scenario briefings (further described in Chapter III) instead of actual OIDs in the *Certificate Policies* field of the X.509 certificate structure.

2. Assumptions

The configuration to be modeled into CyberCIEGE will be an appropriate level of abstraction of PKI implementation that is reflective of real-world deployment, in this way players will not be overwhelmed with unnecessary details that do not contribute to the learning objectives.

For the purpose of this thesis, it is assumed that the PKI setup in CyberCIEGE will operate as per normal, without implementing the details on the life-cycle management of keys, CRL semantics and other fields of the X.509 certificate.

F. SUMMARY

This chapter has described an overview of the key concepts of PKI and the elements to be modeled into CyberCIEGE for this study. The next chapter will present the educational goals and the development strategy of the CyberCIEGE scenario developed as part of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SCENARIO STRATEGY

A. SCENARIO OVERVIEW

As discussed in the previous chapter, end-user awareness and training is essential to realize the true value of any security infrastructure that is put in place by the organization. The next phase of this thesis is thus to develop a CyberCIEGE scenario to portray real-world PKI implementation configurations and teach players the importance of adopting the right configuration to protect the organization’s assets. CyberCIEGE PKI abstractions would be described in terms of player configuration choices and the security implications of these choices on PKI implementation configuration and vulnerabilities.

The intended audience for this CyberCIEGE scenario is IT employees from both the government and corporate sectors. The Federal Public Key Infrastructure (FPKI) has evolved to meet increasing Federal identity management demands, with the emergence of government-wide electronic authentication and identity management guidelines, mandates and standards to promote interoperability of businesses (ICAMSC, 2010). CyberCIEGE complements these efforts by providing a platform to enhance player understanding of PKI choices, trade-offs, and concepts through role-playing the scenario.

As organizations embrace the power of the Internet, e-mail is emerging as an increasingly important communication tool, as it offers a cost-effective way for employees to send business communications to business partners and contractors (Blackbaud, Inc., 2006). Hence, e-mail communications will be an ideal application to illustrate PKI interoperability issues in the scenario developed for this thesis.

The scenario is structured in phases, such that players learn more advanced PKI concepts as they proceed further into the game. Issues concerning certificate revocation and certificate path processing will be presented to the players as they complete each phase sequentially. Changes to the organizational e-mail policy will be introduced incrementally with each phase and players are expected to make the appropriate configuration changes in order to fulfill the objectives to complete that phase. The scenario will be contrived such that players are forced to make certain decisions rather than use brute force and “turn everything on” by default (Irvine & Thompson, 2010).

Players may fail to complete the scenario in the initial attempts, but the scenario is designed to help players learn from the mistakes that they have committed previously. Coupled with the guidance provided through encyclopedia entries and educational videos, players will then be able to understand the various PKI concepts introduced and eventually win the game.

B. DEVELOPMENT OF THE SCENARIO

This section will describe the main storyboard of the scenario and how elements of CyberCIEGE are used to create a game scenario that models realistic PKI deployment issues and a security decision-making process to achieve the educational objectives prescribed for this scenario. The modifications made to the game engine will also be presented along with the development of the scenario.

The first (and recurring) lesson the player must learn is that security policy must be understood: what resources are being protected, and from whom are they being protected? Once the player understands the value (sensitivity) of the resources (information), the player makes choices that affect the protection of the information in accordance with the security policy (Irvine & Thompson, 2003)

In the scenario developed for this thesis, the organizational e-mail policy will be reinforced progressively as the player proceeds through each of the phases and realizes the need for a stronger e-mail policy. It will encompass the key PKI concepts identified in Chapter II, as described in the latter part of this section: use of self-signed certificates, cross-certification, certificate revocation, certificate path processing and X.509 certificate extensions. Players will learn these concepts and appreciate how the PKI settings can be configured securely to ensure strongly authenticated and trusted transactions between a company and her business partners.

A corporate products company, named *Singa Electronic International (Singa)*, will be used as the backdrop for the scenario. The main mode of operations for this company is e-mail exchange of purchase orders and related business data with her official business partner—a manufacturing firm named *Pura Microchip Technology (Pura)*—and its subcontractor named *Friendly Chips (Friendly)*. In the scenario, hostile game characters will be introduced in the form of an employee from a rival company named *Rival Electronics (Rival)*. Assumed to have abundant resources, *Rival's* main aim is to tarnish the reputation of *Singa* by employing technical exploits against ill-configured PKI settings to compromise e-mail assets.

In CyberCIEGE, assets are information resources that may be critical to the organization's success. Assets have value to the organization based on their secrecy or integrity, and assets also have an associated motive value, which determines the means an attacker might employ to compromise the asset. In this scenario, the main assets are the e-mails that contain the details of purchase orders and important business data. *Rival Electronics* is motivated to fool *Singa* and her partners with fraudulent e-mail and thus the player's main aim is to protect the integrity of the e-mail.

Typically, CyberCIEGE scenarios require the player to play the role of a decision maker for a single enterprise. In this scenario, the player will make choices for two enterprises, *Singa* and *Pura*. As part of the scenario briefing and descriptions, the player will be informed of the management policies that were derived based on business relationships between the two enterprises. In particular, *Singa* will accept business transactions that are electronically signed by *Pura*, and *Pura* will accept signed transactions from *Singa*. Both *Singa* and *Pura* have agreed to honor commitments signed using their respective private keys.

To focus the game on the PKI learning objectives, the scenario has some default settings:

- All organizations, together with their respective employees (i.e., users[3]), physical hardware and software components, will be assigned dedicated

[3] "Users" refers to the virtual characters within the game while "players" refer to people who interact with the game simulation.

networks, Discretionary Access Control (DAC) groups and zones with appropriate physical security measures.

- Users will be assigned individual workstations, which have been hardened against typical network attacks.
- All users have gone through the clearance procedures, so players do not have to conduct initial background checks for individual users.

1. Use of Self-Signed Certificates

At the beginning of the scenario, the organizational e-mail policy mandates that all e-mails exchanged between *Singa* and *Pura* will have to be digitally signed with public key certificates to ensure the integrity of the transaction. Hence, the e-mail client software on the users' workstation will be configured with the initial settings that nominally meet this policy. The configurations will instruct the virtual users to sign e-mail with self-signed certificates, and it will instruct virtual users to require e-mail signatures on received e-mail for all e-mail exchanges between *Singa* and *Pura*.

The problem with using self-signed certificates is that this does not offer any guarantee that the identity bound to the particular self-signed certificate is indeed its true owner. In fact, *Rival's* employee could create the following self-signed certificate (as shown in Figure 7) and try to spoof *Singa's* employee's identity by sending an e-mail to *Pura's* employee, requesting for bulk purchase and signing off the e-mail with the self-signed certificate.

Version	**…**	**Issuer**	**…**	**Subject**	**Public Key**
V3	…	*<Singa's employee>*	…	*<Singa's employee>*	RSA (2048 bits)

Figure 7. Sample self-signed certificate structure

Furthermore, the self-signed certificates do not meet the intent of the management policy because they lack a clear tie to the corresponding enterprise. For example, when *Pura* receives a signed order, it needs assurance that the subject who signed the order is indeed an entity that is an authorized representation of *Singa*.

The player would avoid this threat by configuring the e-mail clients of both *Singa's* and *Pura's* employees to "Authenticate certificate." When this option is enabled, the e-mail client will validate the certificate's CA (i.e., the Issuer) against the repository of installed root certificates on the local workstation. In this case, the use of self-signed certificates will fail as none of the Issuers' certificates would be installed as a root on any of the user workstations.

The player learns about the false assurance of using self-signed certificates and that they would fail to authenticate the validity of the entity that is making the representation about the subject of the certificate. Additionally, an encyclopedia entry will be created to explain why self-signed certificates are still used, which form the basis of web of trust in PGP and root certificates in X.509.

In the previous version of CyberCIEGE, the game engine did not distinguish between self-signed certificates and CA-signed certificates. The game engine has been extended to recognize self-signed certificates and is now able to simulate the distinction between authenticating e-mails (purely based on the presence of *any* certificate) and authenticating certificates (validating the *Issuer* against the list of installed root certificates).

2. Cross-Certification

In order to achieve the goal of ensuring that the integrity of the e-mails is not compromised, the player would have to purchase a Certification Authority for both *Singa* and *Pura* and install the root certificate of the newly bought Certification Authority in the respective e-mail clients. The player would then select *Singa's CA* as the Certification Authority for *Singa's* employees and *Pura's CA* as the Certification Authority for *Pura's* employees.

The final step would be the bilateral cross-certification between *Singa's CA* and *Pura's CA* to enable the trust to be extended between users from *Singa* and *Pura*. By allowing the users to achieve the stipulated e-mail goals, the player learns about the cross-certification process and how it enables interoperability of two distinct PKI domains.

The player may choose to install *Singa's CA* as a root certificate on *Pura's* workstations and, correspondingly, *Pura's CA* as a root certificate on *Singa's* workstation. This is still a valid representation that reflects the business policy governing the interoperability of the two domains. However, the management may want the cross-certificates (i.e., the certificate bearing one CA's credentials that is signed by the other CA) to expire in six months, while roots certificates may persist for a longer time.

The player may also opt to subscribe to the services of a public CA, named *Veriscream CA*, by paying it to issue certificates bound to *Singa* and *Pura,* respectively. This means that *Veriscream CA* is now making representation about the identity of the subject of the certificate. In the event that *Veriscream CA* is compromised, *Singa* and *Pura* could not be held liable for the commitments signed using certificates issued by *Veriscream CA*. In the game, the player will encounter the case when the adversary compromises *Versicream CA* to issue bogus certificates that thwart the integrity of the e-mail exchange. The player would then have to revert to the prescribed solution and understand the tradeoffs between using a public CA (more cost-effective, especially for small organizations) and deploying a dedicated CA for the organization (much more resources required, but more secure).

3. Certificate Revocation

Once the player has achieved the first objective in the game, the issue of certificate revocation will be presented to the player. In the real world, there is always the careless employee who would fail to adopt safe key management practices. To support this scenario, the game engine has been modified to simulate exposure of a user's private PKI key and the mitigation of this through the use of a Certificate Revocation List (CRL).

The scenario uses this new feature in the following manner: A careless employee from *Singa* recycled his workstation without clearing his private keys. The adversary was able to get hold of the recycled workstation, gain access to the private key and was able to spoof the identity of the careless employee and e-mail purchase orders on his behalf.

The player would have to purchase a server that stores the Certificate Revocation List (CRL), which would then trigger the IT support staff in the game to revoke the certificate and issue a new one to the careless employee. The *CRL Distribution Point* extension in the X.509 certificate interface will also be updated to reflect the newly purchased server. The player would also have to configure the e-mail clients of the users involved in this part of the scenario to "Check for certificate revocation." When this option is checked, the e-mail client would validate the certificate against the CRL server to ensure that it has not been revoked. The player would thus have to ensure that all the e-mail clients (i.e., the relying parties) would have to be able to connect to the CRL server to check the revocation status of a certificate. This would then prevent the attacker from continuing to use the exposed private key of the careless employee.

Through this scenario, the player learns about the importance of certificate revocation and the consequence of not implementing it as part of the PKI when he/she sees the actualization of an attack where the adversary uses the private key maliciously.

4. Certificate Path Processing

After the completion of Phase 1 of the scenario, the organizational e-mail policy would have been reinforced to include additional requirements (which correspond to the PKI concepts presented in the previous phase of the scenario):

- The use of self-signed certificates shall be prohibited.
- All certificates shall be authenticated against the repository of installed root certificates.
- All certificates shall be checked against the CRL repository.

Phase 2 of the scenario is designed with the intent to help the player understand how certificate path processing is related to certificate policies—which reflects actual business relationships—especially when two or more organizations are involved. In this phase, the player is required to accomplish a new objective, which is to ensure that *Singa's* employees are able to authenticate e-mail orders from *Friendly*, the subcontractor of *Pura*. This is a realistic representation of the operational considerations that organizations in the real world face, when they have to ensure the interoperability of their PKI with other PKIs to meet certain business requirements.

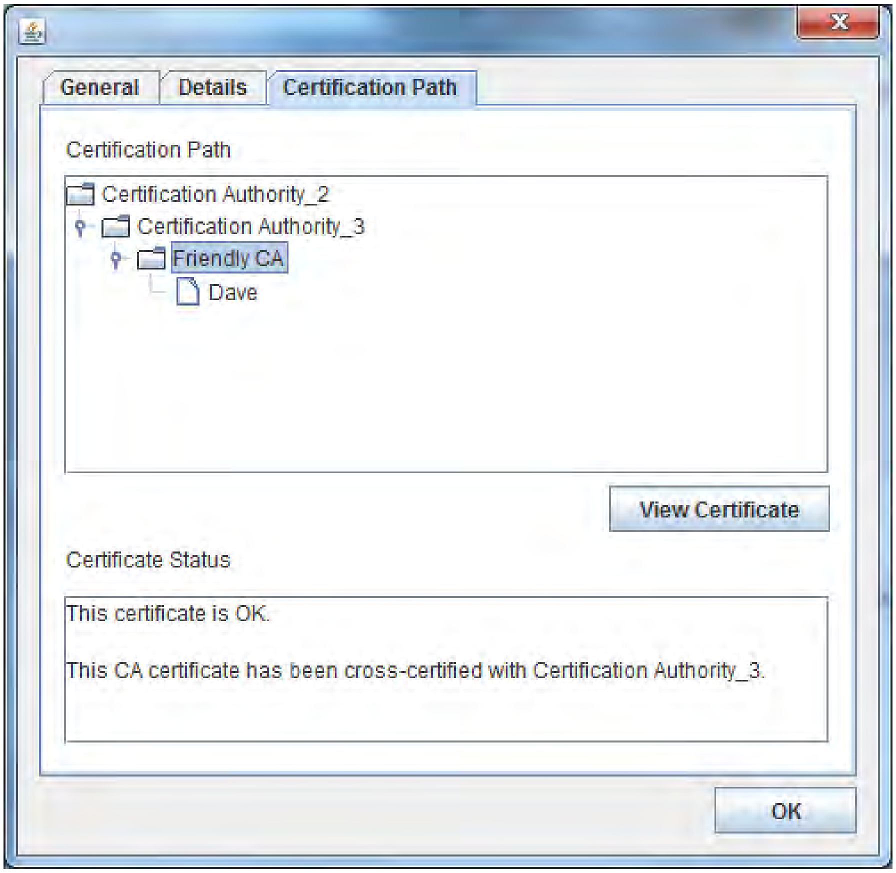
According to the settings that the player has configured thus far from the beginning of the scenario, *Singa's* employees are not able to validate any of *Friendly's* employees' certificates, because *Friendly's CA* has not been installed as a root certificate in *Singa's* workstations, nor has it been cross-certified with *Singa's CA* or *Pura's CA*. The initial scenario briefing will present instructions to lead the player to configure *Pura's CA* to cross-certify[4] *Friendly's CA* certificate, since *Friendly* is *Pura's* subcontractor and the two organizations would have established formal agreements on certificate usage policies.

If this is done correctly, the users in the game would be able to achieve their e-mail goals and the player would then be able to proceed to the next phase of the scenario. The player would also be presented with a multiple-choice question at the end of the scenario to test if they have understood how the certificate chain was constructed and validated, hence enabling e-mail exchange between *Singa* and *Friendly*.

In addition, the player could click on "Validate Certificate" to view the validation results or visually verify and trace the certificate chain through the enhanced X.509 certificate interface (as shown in Figure 8) and understand how the certificate of

[4] This is an example of a unilateral cross-certification, where Pura's CA signs Friendly's CA certificate, but not vice versa. Unilateral cross-certification suffices to meet the objective prescribed for this phase of the scenario.

Friendly's employee was validated. In making the necessary configuration change and answering the question correctly, the concept of certificate path processing would be reinforced.



Certification Path

- Certification Authority_2
  - Certification Authority_3
    - Friendly CA
      - Dave

Certificate Status

This certificate is OK.

This CA certificate has been cross-certified with Certification Authority_3.

Figure 8. X.509 certificate interface showing certification path

There are a few ways the player could make configuration changes in order to let the users achieve the e-mail goals. For example, the player could choose to configure *Singa's CA* to cross-certify *Friendly's CA* certificate, or just install *Friendly's CA* certificate as a root certificate in *Singa's* workstations. This however, does not conform to the policy that was being described via the scenario briefings. As discussed in Chapter II Section C2, certificate policy terms dictate specific requirements for certification paths that include the CA certificate. In this case, it is important that the player understands that *Pura's* signing of *Friendly's* certificate indicates the representation that *Pura* has established customer agreements and terms of use with *Friendly* as her subcontractor. *Singa* is relying on this representation made by *Pura* and *Singa* has business recourse in the event of a misrepresentation. If the player made any of the alternate configurations, Singa would not have recourse against Pura in the event that Friendly's CA certificate is subverted.

Nevertheless, the player will not be penalized and forced to revert to the prescribed solution, but instead his/her understanding will be challenged till he/she obtains the correct answer for the multiple choice question. Additionally, an encyclopedia entry will be created to present the different possible options of enabling interoperability between organizations and their respective tradeoffs.

5. Key Usage

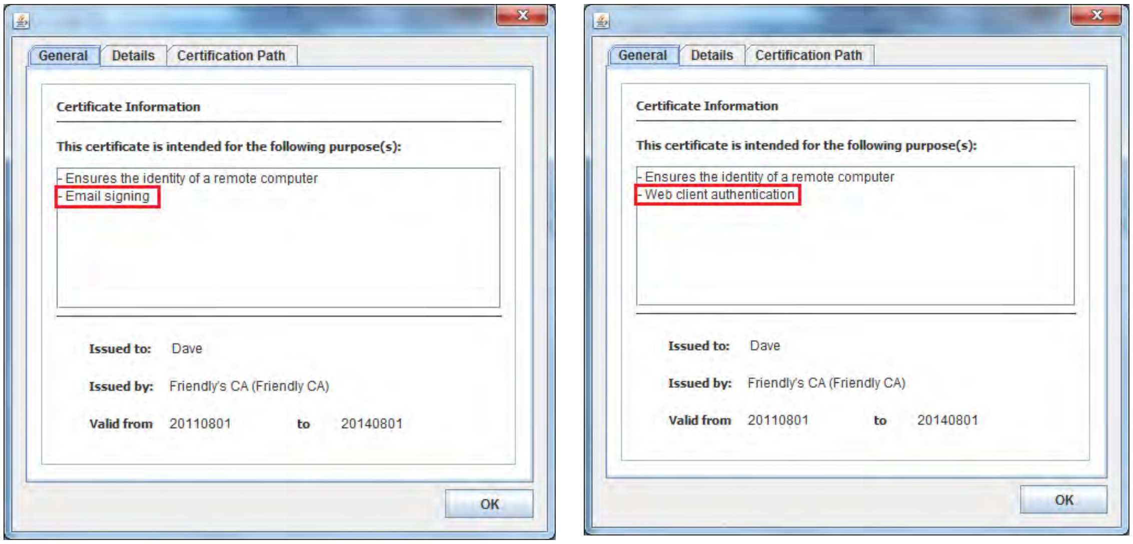
The final phase of this scenario challenges the player with a new requirement to allow *Singa's* employees to place purchase orders via *Rival's* webpage to secure a rare microchip that only *Rival* produces, while protecting the integrity of the transactions with their other partners.

The player would be required to set up a Transport Layer Security (TLS) web client authentication to allow *Singa's* employees to access *Rival's* webpage to place the required purchase orders. The TLS authentication procedure will specifically involve the server sending a random challenge string for the client to sign with his private key; the server will then be able to validate the response using the client's public key in order to authenticate the client. When the player first configures the TLS web client settings on *Singa's* workstations, the game engine has been programmed to entice him/her to reuse the existing e-mail certificate when *Singa's CA* is chosen to be the Certification Authority. Next, the TLS challenge response will be specially crafted (e.g., "*Singa* would like to place 1,000,000 orders of Microchip M with *Pura*.") to cause *Singa's* employee to "sign" it unknowingly during the authentication procedure.

The game engine has been modified to understand the notion of the digital signing key and identity key and will simulate the following attack by *Rival*. *Rival's* employee spoofs *Singa's* employee's identity by specially crafting a separate e-mail with the same body content "*Singa* would like to place 1,000,000 orders of Microchip M with *Pura*." appends the authentic signature obtained from the above authentication procedure and sends it to *Pura*. With a valid certificate issued by *Singa's CA* to *Singa's* employee that has not been revoked, *Singa* is not able to repudiate this e-mail and hence must honor the bogus order.

The vulnerability that the adversary tries to exploit in this scenario is the failure to distinguish between the key used for digital signing and the one used for identification. To counter this threat, the player would have to generate a separate certificate and key pair specifically for identification purpose. The TLS web client settings would also have to be configured to use the newly-generated identity certificate for authentication. In this way, *Rival* would not be able to extort *Singa* with the signed malicious response, since it has been signed with an identity key and not a signing key.

Additionally, the player could visually verify the purpose of the different types of certificates available in the scenario through the enhanced X.509 certificate interface (as shown in Figure 9) and note the subtle difference between a certificate used for digital signing and one used for identification.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Email signing

Issued to: Dave

Issued by: Friendly's CA (Friendly CA)

Valid from 20110801 to 20140801

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Web client authentication

Issued to: Dave

Issued by: Friendly's CA (Friendly CA)

Valid from 20110801 to 20140801

Figure 9. X.509 certificate interface showing certificate purpose

Through this scenario, the player would be able to note the subtleties involved when PKI is used in TLS client authentication and learn how attackers make use of these to overcome security controls.

Once the player has met all the objectives prescribed in each phase of the scenario, he/she would then be able to complete and win the scenario. At the end of the game, the player would have picked up the key concepts of PKI, understood some real-world deployment issues and recognized the implication of certain security decisions he/she made as a security administrator.

C. SUMMARY

This chapter has presented the design of a CyberCIEGE scenario that models realistic PKI deployment issues and security decision-making processes that help to achieve the learning objectives prescribed for this PKI study. The next chapter will provide more detail on how the various elements available in CyberCIEGE were used to implement the actual scenario.

IV. SCENARIO DESCRIPTION

As part of this thesis research, a CyberCIEGE scenario named *Cert Attack* was developed to model realistic PKI deployment issues and a security decision-making process to achieve the educational objectives set out in Chapter II Section B. This chapter will describe the details of implementing the scenario in accordance with the strategies that have been outlined in Chapter III.

A. SCENARIO BRIEFING

The purpose of the briefing is to provide the player with a summary of the information security policy, which in this case is centered on maintaining the integrity of e-mail assets. The briefing is intended to inform the player that the e-mail content is relied upon by both organizations and thus the management has established strong security policies to ensure that all e-mails are digitally signed by people who are authorized representatives of *Singa* and *Pura*. The policy description within the briefing is further augmented by descriptions of the scenario assets and descriptions of objectives.

The following is the in-depth description of the scenario setting, which provides a description of the scenario context, the goals and requirements for the player and the instructions to play the game:

> Welcome to *Singa Electronic International*. To enable *Singa* to produce the finest electronics in the region, *Singa's* management has established business agreements to order microchips exclusively with her official partner, *Pura Microchip Technology*. As part of the security policy, *Singa* and *Pura* have consented to using PKI to ensure the integrity of the transactions between the two organizations. In particular, *Singa* will accept business transactions that are electronically signed by *Pura*, and *Pura* will accept signed transactions from *Singa*. Both *Singa* and *Pura* have agreed to honor commitments signed using their respective private keys.
>
> You have been appointed the Chief Information Security Officer (CISO) and will be responsible for providing the necessary infrastructure to *Singa* and *Pura* to protect the integrity of the e-mail assets, such that they will

not be subject to attacks by *Rival Electronics*, *Singa's* greatest competitor. As the CISO, you will need to understand the goals of the users, make decisions about the types of physical components to be purchased and how to configure these components. You will also need to take note of the individual policies *Singa* and *Pura* have while making these configuration choices. If your choice of implementation compromises the security of the e-mail assets in *Singa*/*Pura*, you will suffer monetary penalties. If you are able to fulfill all the objectives without encountering security attacks, you will proceed to the next phase of the game. You win the game once you have successfully completed all the objectives.

This scenario is divided into three phases. You must complete all objectives of a phase before proceeding to the next phase. Use the "OBJECTIVES" tab to review your objectives for each phase. Press "F1" at any time to launch the encyclopedia. Press "k" to view keyboard shortcuts and navigation keys. Once you are ready, click the "OFFICE" tab and click the green button to play the game. Good luck!

B. ZONE LAYOUT AND INITIAL NETWORK CONFIGURATION

The scenario consists of the main zone, which is the office of *Singa Electronic Limited*, three offsite offices, namely *Pura Microchip Technology, Friendly Chips* and *Rival Electronics*, and a web zone where the public Certification Authority *Veriscream CA* resides. The layout of the scenario is shown in Figure 10.

The player has been assigned the role of a CISO and will be responsible for configuring and maintaining the infrastructure in *Singa Electronic Limited* and *Pura Microchip Technology*. The player will not be able to configure the components residing in other zones.

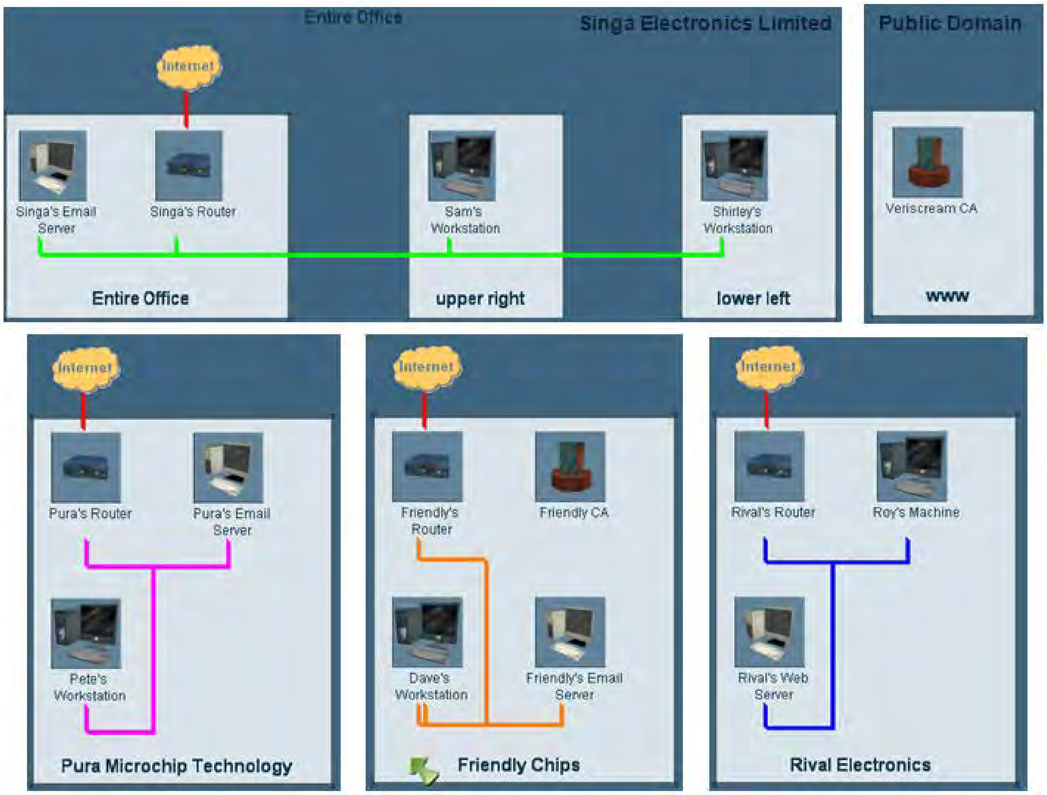


Figure 10. Layout of *Cert Attack* scenario

C. USERS AND USER GOALS

Users are the virtual characters within CyberCIEGE. If computers are available and purchased by the player, users will create and access the assets using the computers. User behavior is driven by the user goals specified by the scenario designer (CISR, 2011). If user goals are not met, the users will express frustration and their productivities will be affected, which adversely affects the success of the organization. User goals can thus be used as a means to determine if the player has deployed the right infrastructure and configured the necessary settings, and will be used to decide if the player has achieved the game objectives.

In the *Cert Attack* scenario, there are five users: Shirley and Sam from *Singa Electronic Limited*, Pete from *Pura Microchip Technology*, Dave from *Friendly Chips* and Roy from *Rival Electronics*.

Shirley is the primary liaison officer in *Singa Electronic Limited*. She is in charge of issuing purchase orders on behalf of *Singa* to Pete of *Pura Microchip Technology*. She also reads the technical specifications and any related business data sent by Pete and Dave of *Friendly Chips*. She is also tasked to place purchase orders from *Rival Electronics'* web page to procure a rare chip. Shirley must be able to send e-mails to Pete, receive e-mails from Pete and Dave and access *Rival's* webpage in order to fulfill her user goals.

Sam is the secondary liaison officer in *Singa Electronic Limited*. He is responsible for issuing purchase orders on behalf of *Singa* to Pete, when Shirley is away from office. He needs to be able to send e-mail to Pete to complete his job. In this scenario, Sam is notorious for his sloppiness with regard to safe security practices.

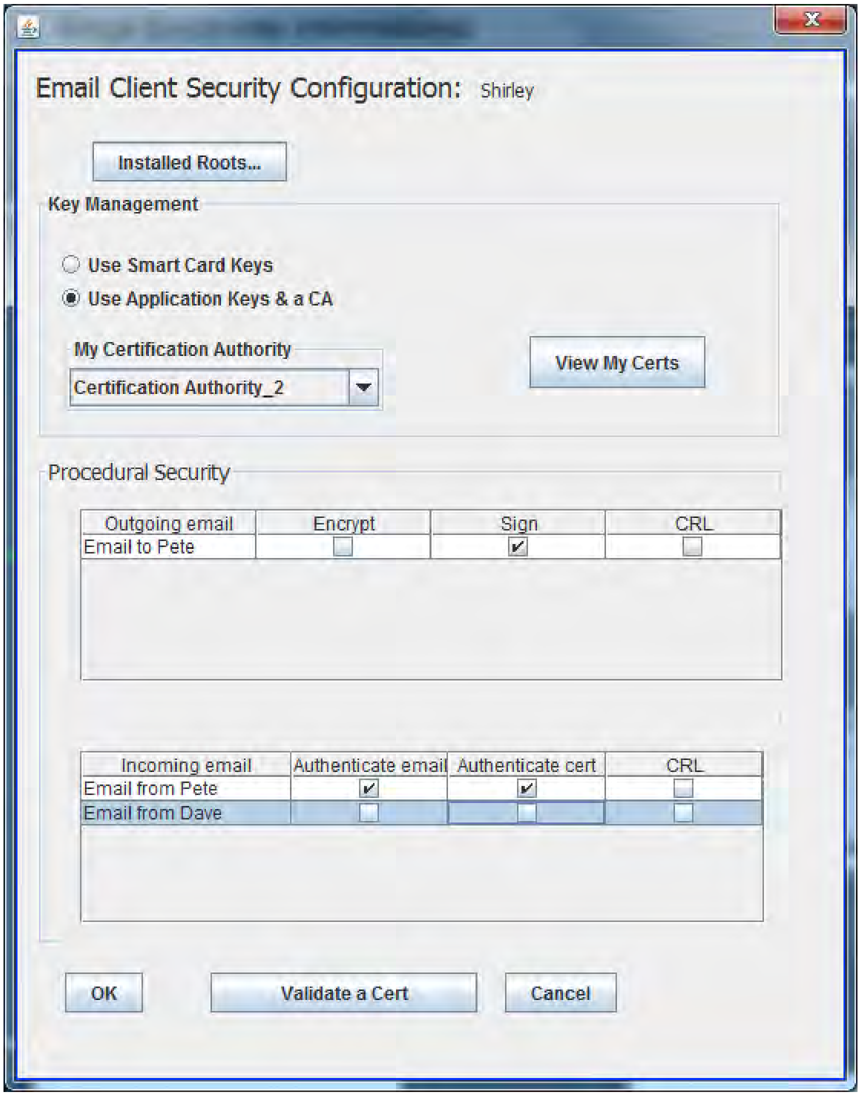
Pete is the main liaison officer in *Pura Microchip Technology*. He is in charge of accepting and processing purchase orders on behalf of *Pura* from Shirley/Sam. Pete must be able to send e-mails to Shirley, and receive e-mails from Shirley and Sam in order to accomplish his goal.

Dave is an employee of *Friendly Chips*, the official subcontractor of *Pura*. He is responsible for sending technical specifications on behalf of *Pura* to Shirley for her review. Dave needs to be able to send e-mails to Shirley to fulfill his job requirement.

Roy is a highly skilled hacker employed by *Rival Electronics*. Equipped with abundant resources and knowledge, his main aim is to tarnish the reputation of *Singa*. Although Roy has not been assigned any explicit user goals, he will constantly attempt to employ technical exploits against ill-configured PKI settings of *Singa* and *Pura* in order to compromise e-mail assets.

D. PHYSICAL COMPONENTS

The scenario is first loaded with the physical components as shown in Figure 10. The users are seated in their respective zones and are assigned individual workstations, which have been hardened against typical network attacks. Each workstation can be configured with distinct application settings; in particular, e-mail and browser SSL settings (see Figures 11 and 12, respectively), which the player has to update in order to complete the objectives of the game.



Email Client Security Configuration: Shirley

Installed Roots...

Key Management

○ Use Smart Card Keys

● Use Application Keys & a CA

My Certification Authority: Certification Authority_2

View My Certs

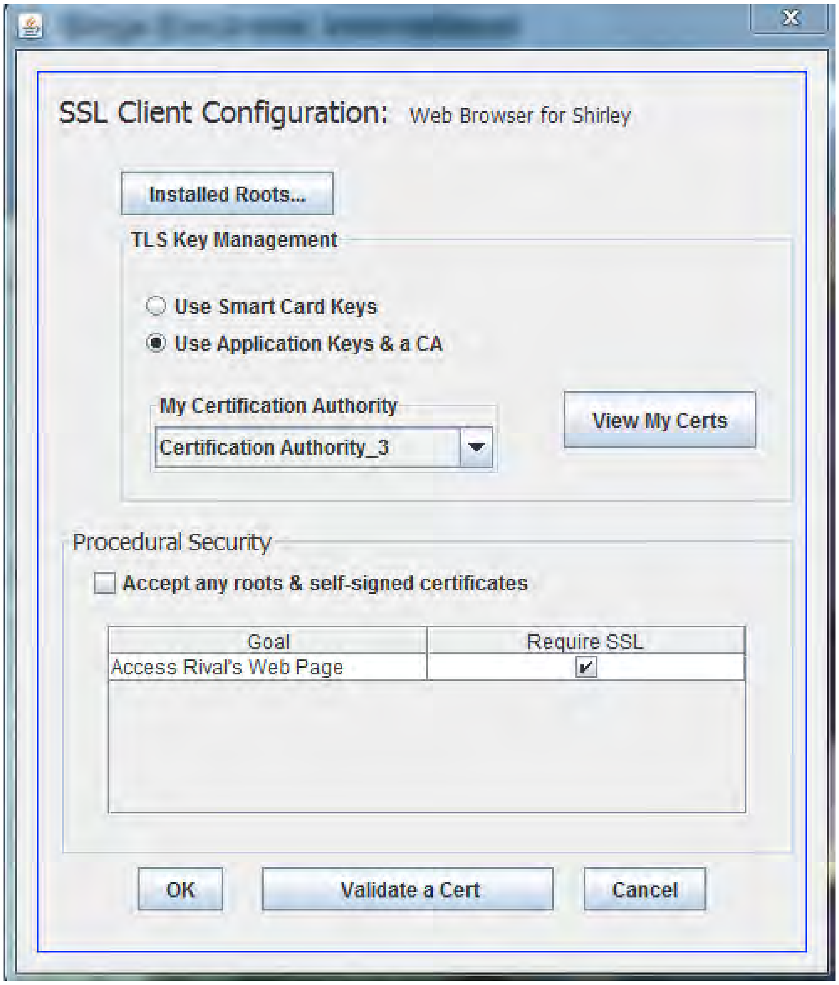
Procedural Security

Outgoing email	Encrypt	Sign	CRL
Email to Pete	□	☑	□

Incoming email	Authenticate email	Authenticate cert	CRL
Email from Pete	☑	☑	□
Email from Dave	□	□	□

OK · Validate a Cert · Cancel

Figure 11. E-mail Client Security Configuration interface



[redacted]

SSL Client Configuration: Web Browser for Shirley

Installed Roots...

TLS Key Management

○ Use Smart Card Keys

● Use Application Keys & a CA

My Certification Authority: Certification Authority_3

View My Certs

Procedural Security

□ Accept any roots & self-signed certificates

Goal	Require SSL
Access Rival's Web Page	☑

OK Validate a Cert Cancel

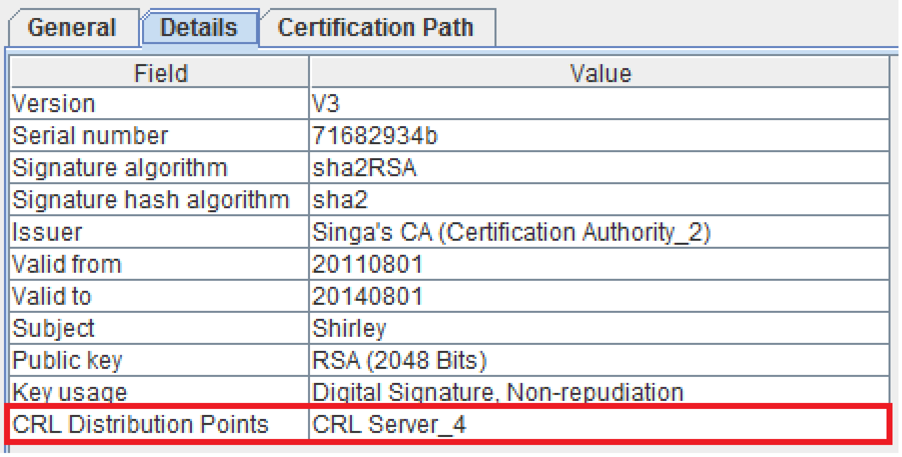
Figure 12. SSL Client Configuration interface

Every zone has a router that connects all the workstations and servers of that particular organization to the Internet. E-mail servers are deployed in *Singa's, Pura's* and *Friendly's* zone to enable Sam, Shirley, Pete and Dave to exchange e-mails to fulfill their user goals. A web server is deployed in *Rival's* zone to host *Rival's* webpage, which Shirley will need to access as part of her job requirement. Two Certification Authorities are set up in *Friendly's* zone and the web zone, respectively. *Friendly CA* is configured to be the Certification Authority for Dave. *Veriscream CA* is a public CA that resides in the web zone and issues pay-per-use certificates. It is the CA for Rival's web server.

All the physical components in Friendly's, Rival's and the web zone are static components, i.e., the player will not be able to configure these components.

The player will have to purchase some additional PKI components and deploy them onto the respective networks in order to achieve the objectives of the scenario. The catalog of components that are available for the players to purchase is as follows:

- CRL Server. This is a high-cost specialized server that stores the certificate revocation. Once deployed, the IT support staff will revoke the certificate that has been compromised. It will also be reflected as the CRL Distribution Point in the X.509 certificate interface (see Figure 13).



Field	Value
Version	V3
Serial number	71682934b
Signature algorithm	sha2RSA
Signature hash algorithm	sha2
Issuer	Singa's CA (Certification Authority_2)
Valid from	20110801
Valid to	20140801
Subject	Shirley
Public key	RSA (2048 Bits)
Key usage	Digital Signature, Non-repudiation
CRL Distribution Points	CRL Server_4

Figure 13. X.509 certificate interface showing CRL Distribution Point

- Certification Authority. This is a specialized server that contains certification authority software (not unlike much of the real world). Some scenarios include public "pay-per-cert" CAs that issue certificates. Players also have the option to purchase their own CAs to issue certificates for PKI-enabled components and applications.

E. NETWORKS

Each zone will be assigned its individual network, which will connect all physical components in that zone, except for Friendly, CA, which will remain standalone, to reduce its exposure to Internet attacks that aim to subvert Certification Authorities. All the zones are connected to the Internet by default, so as to allow intercommunications between the different companies.

F. ASSETS

In CyberCIEGE, assets are resources. Players succeed by facilitating user access to assets. Assets are tagged with a *motive*, which determines the *means* by which the attacker will attempt to compromise an asset. Player choices affect the *opportunity* for the attacker to compromise the assets. The enterprise (and by extension the player) is penalized the value of an asset should it be compromised or made unavailable (CiSR, 2011).

E-mails are the most important assets in *Cert Attack*, since all business transactions occur via e-mail communications. As discussed in Chapter III, both *Singa* and *Pura* will honor the commitment to purchase orders sent via e-mail and hence the e-mail assets are very valuable to both organizations. These are characterized by the following assets in the scenario: E-mail from Shirley to Pete, E-mail from Pete to Shirley and E-mail from Sam to Pete. These assets have to be authenticated against the sender of the e-mail, such that the recipient will have recourse against the sender. The later part of the scenario will require Dave to send technical specifications for a particular microchip to Shirley on behalf of Pete. This e-mail from Dave to Shirley will also have to be validated to uphold the trust in the e-mail communications that *Singa* and *Pura* have achieved and maintained thus far.

In Cert Attack, the attacks are driven by the motives that relate to the integrity of the e-mail assets. This means that successful modification or impersonation of this asset (by the attacker) will result in monetary penalties. All e-mail assets have *motive* values of

50 to attract potential attackers like Roy. E-mail assets are stored in the e-mail servers residing in *Singa's*, *Pura's* and *Friendly's* zones, respectively.

G. PHASES AND OBJECTIVES

This scenario is divided into three phases, with each phase introducing to the players some key concepts of PKI. There is a set of objectives tied to each phase of the scenario and the player is expected to fulfill the objectives by demonstrating knowledge of the PKI concepts being challenged.

Phase 1 introduces the notion of self-signed certificates, cross-certification and certificate revocation. The player has to configure the e-mail client settings of the workstations of *Singa* and *Pura* and purchase the appropriate PKI components to ensure that Roy is not able to fool Shirley, Sam and Pete with fraudulent e-mails.

Phase 2 introduces the concept of certificate path processing. The player is required to accomplish a new objective—to ensure that Shirley is able to receive business data from Dave. The key to completing this phase is to ensure that the player understands why the users in the game can achieve their e-mail goal by answering the questions posted at the end of this phase correctly.

Phase 3, the final phase, extends the secure communications requirement from only e-mail, to include webpage (*Rival's*) access. In this case, Rival's webpage is simply a contrivance to confront the player with a security decision on the choice of keys, i.e., it is an *asset* that has not been assigned any motive value to entice Roy to compromise the actual webpage access. Roy is, however, motivated to entice Shirley to sign a malicious challenge string which he can use it to craft a bogus e-mail to spoof the asset "E-mail from Shirley to Pete". Hence to win the game, the player needs to comprehend the subtle difference between a digital signing key and an identity key and make the right configuration to ensure that Shirley can place orders securely on *Rival's* webpage without Roy being able to compromise any of the e-mail assets.

H. QUESTIONS

In CyberCIEGE, question triggers can be used to test a player's understanding of material and to potentially alter the direction of a scenario (CISR, 2011). The response to an incorrect player answer can be uniquely defined and the player will be required to answer the question again until he/she selects the correct reply.

In Phase 2 of the *Cert Attack* scenario, the player's understanding will be challenged via a multiple choice question (displayed in Figure 14) to check if he/she has understood the concept of certificate path processing, even though he/she may have configured the game settings incorrectly.

<table>
<tr><td colspan="3"><b>Question</b>: What do you think is the correct way to permit Shirley to authenticate e-mails from Dave, based on Singa's company policy?</td></tr>
<tr><td colspan="2"><b>Answer</b></td><td><b>Feedback to Player</b></td></tr>
<tr><td>a.</td><td>Configure Shirley's workstation to accept self-signed certificates and direct Dave to use self-signed certificates.</td><td>Incorrect.
The use of self-signed certificates was disallowed after the first attack by Roy.
Please try answering the question again.</td></tr>
<tr><td>b.</td><td>Install Friendly CA's (Dave's CA) certificate as a trusted root in Shirley's workstation.</td><td>Incorrect.
Installing Friendly CA's certificate as a trusted root certificate in Shirley's workstation will enable Shirley to authenticate e-mails from Dave, but this is against Singa's company policy, as stated in the scenario briefing. In this case, Singa would have no recourse against Pura in the event that Friendly's CA certificate is subverted.
Please try answering the question again.</td></tr>
<tr><td>c.</td><td>Sign Friendly CA's (Dave's CA) certificate with Singa's CA, which is already a trusted root installed in Shirley's workstation.</td><td>Incorrect.
Signing Friendly CA's certificate using Singa's CA will enable Shirley to authenticate e-mails from Dave, but this is against Singa's company policy, as stated in the scenario briefing. In this case, Singa would have no recourse against Pura in the event that Friendly's CA certificate is subverted.
Please try answering the question again.</td></tr>
</table>

Question: What do you think is the correct way to permit Shirley to authenticate e-mails from Dave, based on Singa's company policy?		
Answer		**Feedback to Player**
d.	Sign Friendly's CA (Dave's CA) certificate with Pura's CA, whose CA has been cross-certified with Singa's CA, which is a trusted root installed in Shirley's workstation.	Correct. As stated in the scenario briefing, Pura's signing of Friendly CA's certificate indicates the representation that Pura has established customer agreements and terms of use with Friendly as her subcontractor. Singa can then rely on this representation made by Pura and have business/legal recourse in the event of a misrepresentation.

Figure 14. CyberCIEGE question form for *Cert Attack*

I. CONDITIONS AND TRIGGERS

The CyberCIEGE scenario definition language allows scenario designers to periodically assess the ongoing game state "conditions" and respond using active "triggers" (CISR, 2011). Conditions can be used to assess whether players have achieved the game objectives or to provide the player with feedback before the engine does harm to the player's network. Upon the occurrence of these conditions, the CyberCIEGE game engine will execute the corresponding triggers, which include popup messages, encyclopedia help entries, changes in user goals, commencement of attacks and user feedback to the player via balloon speech.

The following section highlights some of the conditions and triggers that have been defined to measure the player progress and to provide appropriate feedback to the player for the *Cert Attack* scenario:

<u>Shirley has authenticated Pete's certificate</u>. This condition checks if the player has completed the first objective for Phase 1. In order to satisfy this condition, Shirley and Pete must have uninterrupted access to the respective assets without successful attacks by Roy for a specified period of time. This means that the player has to purchase additional CAs for *Singa* and *Pura*, as well as configure the e-mail settings of Shirley and Pete to allow them to exchange e-mail securely without Roy being able to carry out spoofed e-

mail attacks in the specified time frame. When this condition is satisfied, a popup message will also be triggered to inform the player of his/her next objective.

Sam’s certificate got compromised. In the second part of Phase 1, the scenario directs the game engine to simulate the case when Sam’s workstation is discarded without clearing the private keys, which subsequently fall into Roy’s hands. A *KeyExposed* trigger is used to simulate the exposure of Sam’s private key. Attack triggers are defined to go off at a predefined interval (further discussed in “E-mail Attacks or Internet Attacks”), and the next spoofed e-mail attack will succeed unless the player has taken steps to effectively revoke Sam’s certificate., A successful attack then triggers Roy to describe how the attack on the asset “E-mail from Sam to Pete” took place. Sam’s old certificate has been revoked. This condition verifies if the player has completed the second objective for Phase 1. To satisfy this condition, the player has to deploy a CRL server and direct Pete to check CRLs when authenticating e-mail from Sam to mitigate the attack caused by the *KeyExposed* trigger. If this condition is met, the player would have completed all the objectives in Phase 1 and the scenario will proceed to the next phase.

Shirley installs *Pura’s CA* as root and/or Pete installs *Singa’s CA* as root. This condition checks if the player has misinterpreted the organizational policy described in the scenario briefing and installs *Singa’s CA*/*Pura’s CA* as a trusted root in Pete/Shirley’s workstation, respectively. If this condition is true, it means that the player has not fully understood the notion of cross-certification and will be required to revert to the prescribed solution in order to meet the objective of Phase 1.

Shirley installs *Friendly’s CA* as root or *Singa’s CA* signs *Friendly CA*’s certificate. This condition checks if the player has misinterpreted the organization policy described in the scenario briefing and installs *Friendly CA* as a trusted root in Shirley’s workstation or has misconfigured *Singa’s CA* to sign *Friendly CA’s* certificate. If either of these conditions occurs, a different question dialog will be triggered to differentiate the feedback to the player when he/she answers incorrectly (as a result of his/her misconfiguration).

Shirley has received Dave's e-mail. This condition verifies if the player has completed the objective for Phase 2, i.e., to allow Shirley to receive and authenticate e-mails from Dave. The player will have to demonstrate that he/she has understood how the business policy influenced the way the certificate path should be processed, by answering the question correctly. This is the goal and objective for Phase 2 of *Cert Attack*. If this condition is satisfied, the game will proceed to the final phase.

Install *Singa's CA* as root on *Rival's* web server. In the final phase, Shirley will need to access *Rival's* web page via a TLS web session. This trigger will instruct the game engine to install the CA's root certificate that the player has purchased for *Singa* as a trusted root on *Rival's* web server in order to allow TLS web session. Otherwise, *Rival's* web server will not be able to validate Shirley's identity and hence fail the user goal.

Shirley is able to access *Rival's* web page. This condition checks if the player has fulfilled the objective for Phase 3. To satisfy this condition, the player has to allow Shirley to access *Rival's* web page via a TLS web client session, without exposing any vulnerability that Roy can exploit. If this condition is true, the player would have completed all the objectives of the scenario and win the game.

E-mail Attacks or Internet Attacks. The game engine determines the success of attacks based on attacker motive, network topology, configuration settings and procedural settings (CISR, 2011). The "E-mail Attacks" and "Internet Attacks" triggers are defined such that the game engine derives attacker motive from the individual asset motives (discussed in Section F), and will cause the game engine to launch spoofed e-mail attacks or Internet attacks with a frequency of 0.04 days. If any of the e-mail assets has not been protected, the attack will succeed and the *AssetAttacked* condition will evaluate to *true*.

The objectives described above are marked as complete by triggers that evaluate *AssetAttacked* conditions as well as conditions that assess user goal failures. The evaluation period of these triggers is 0.05 days. If attacks did not occur and users have had uninterrupted access to assets for 0.05 days, it implies the player has implemented the necessary countermeasures to prevent the attacks from happening.

When any of the attack happens, speak triggers will be invoked and Roy will describe the details of his attack on the game screen.

J. SUMMARY

This chapter provided details on how the Cert Attack scenario was designed and implemented using the elements of CyberCIEGE. The extensive features of CyberCIEGE allowed intelligence and attack logic to be built into the game, which enabled the development of this scenario to portray real-world PKI implementations and let the players recognize the implication of their own security decisions.

The next chapter will cover the test objectives and strategies to verify the correctness of the *Cert Attack* scenario as well as provide a walkthrough on the proposed solution to the scenario.

V. SCENARIO TESTING

This chapter describes the test methodology applied for the *Cert Attack* scenario. Details of the testing scope, expected results and actual results of each test case are also documented.

A. TEST METHODOLOGY

The main objective of this test is to demonstrate that the Cert Attack scenario can reasonably portray real-world PKI implementations, and that the simulation feedback to the player as he/she progresses in the game is consistent with real-world behavior to fully enhance the learning experience of the player.

Test cases were designed to verify the flow of the scenario, such that the feedback provided in the simulation were logical and realistic as the player interacted with the game engine. The intention of this testing is not to be exhaustive and provide complete coverage for all edge test cases, but to ensure that the Cert Attack scenario continues to run as expected when new changes are introduced to the CyberCIEGE game engine in the future.

Test procedures were developed by utilizing the game logging function, which logs each game event that occurred during the course of playing a scenario. After a scenario has been played, the resulting log can be replayed, such that the game automatically executes the click/key sequences necessary to get to a desired point within a scenario (CISR, 2011). In this way, test procedures can be repeatedly run against the game engine via these replay logs.

Each test case corresponded to a game objective that was discussed in Chapter IV. The test cases were designed to be incremental, i.e., the test case for the next game objective depended upon the execution of the correct test sequence for the previous test case. The scenario was then executed according to the procedures defined in each test case and the actual results were observed and recorded. Every test was executed on the same version of CyberCIEGE game engine to ensure consistency.

For each test case, two categories of tests were considered. First, the scenario was tested with the desired game moves necessary to achieve the goal of the scenario. In this case, the player would receive positive feedback and advance to the next phase of the game. The second category of test cases involved anticipated alternative or incorrect game moves. In this case, the player made bad security decisions and configured the game components differently, hence deviating from the prescribed solution. The game would present negative feedback to either hint the player to reconfigure the components or to reinforce the players' understanding on certain PKI concepts by allowing them to proceed only when they have answered the quiz correctly.

B. TEST CASES

This section presents four sets of test cases that were derived. The first part of the test case defines the scope of the test case as well as the procedures required to achieve the expected results, which forms the next part of the test case. The final part records the actual results observed from running the game against the test case. These results will be compared with the expected results to see if the test succeeds.

1. Test Case 1: Authentication of Pete's Certificate

a. Scope of Test Case

Test Case 1 corresponds to the first objective in Phase 1 of Cert Attack, which introduces the concept of self-signed certificates and cross-certification. At the start of the scenario, Shirley and Pete have been preconfigured to exchange e-mails using self-signed certificates, which will subject themselves to spoofed e-mail attacks by Roy. Therefore, the player has to perform the following procedures in the game:

i) Purchase a Certification Authority for *Singa* and place it in the server room at *Singa's* office.

ii) Purchase a Certification Authority for *Pura* and place it in the server room at *Pura's* office.

iii) Right click on *Pura's CA* and configure it to sign *Singa's CA*.

iv) Right click on *Singa's CA* and configure it to sign *Pura's CA*.

v) Hire an additional IT support staff to manage the *Singa's CA* and *Pura's CA*.

vi) Right click on Shirley's workstation and configure her e-mail application settings:

- Select "*Singa's CA*" as her Certification Authority.
- Add "*Singa's CA*" to her list of installed roots.
- Check "Authenticate Certificate" for "E-mail from Pete" under Incoming e-mail procedural settings.

vii) Right click on Pete's workstation and configure his e-mail application settings:

- Select "*Pura's CA*" as his Certification Authority.
- Add "*Pura's CA*" to his list of installed roots.
- Check "Authenticate Certificate" for "E-mail from Shirley" under Incoming e-mail procedural settings.

b. Expected Results

If the player follows the procedures listed in the previous subsection, the scenario will proceed to the next part of Phase 1. If the player executes any incorrect move, he/she may not be able to achieve the objective, as summarized in Table 2.

Table 2. Test Case 1 Expected results

Test ID	Description	Expected Results
1a	The player executes the game sequence as described in Section B1a. (Note: The order by which steps iii-vii is to be performed does not matter.)	Shirley and Pete will fulfill their objectives to exchange trusted e-mails.
1b	The player chooses the public *Veriscream CA* instead of purchasing CAs for *Singa* and *Pura*, selects it as Shirley's and Pete's Certification Authority and adds it to their list of installed roots. The player also checks the "Authenticate Certificate" option.	Shirley and Pete will be able to exchange e-mails, but the e-mails will be spoofed by Roy.
1c	Instead of performing cross-certification via steps i-iv, the player chooses to add *Singa's CA* to Pete's list of installed roots and *Pura's CA* to Shirley's list of installed roots.	Shirley and Pete will be able to exchange trusted e-mails and will not be susceptible to Roy's attacks, but the player will fail the objective because this deviates from the company policies of Singa and Pura, as stated in the scenario briefing.

c. Actual Results

Table 3 documents the actual results and checks if they meet the expected results.

Table 3. Test Case 1 Actual results

Test ID	Actual Results	Meets Expected Results?
1a	Shirley and Pete achieved their goals.	Yes
1b	Shirley and Pete could exchange e-mails, but the e-mail's integrity was compromised by Roy. As a result, the player incurred monetary penalties.	Yes

Test ID	Actual Results	Meets Expected Results?
1c	Shirley and Pete could exchange trusted e-mails, but the game did not proceed to the next objective and displayed a popup message informing the player to review the policy in the scenario briefing.	Yes

2. Test Case 2: Revocation of Sam's Old Certificate

a. Scope of Test Case

Test Case 2 corresponds to the second objective in Phase 1 of Cert Attack, which introduces the notion of certificate revocation. A preconfigured trigger will simulate the exposure of Sam's private key, which Roy will use to send spoofed e-mails to Pete. Therefore, the player has to perform the following procedures to resolve this issue:

i) Purchase a CRL server for *Singa* and place it in the server room at *Singa's* office. This action will trigger the IT support staff to revoke Sam's certificate.

ii) Connect the CRL server to "Lan 1" (*Singa's* network).

iii) Right click on Sam's workstation and configure his e-mail application settings:

- Select "*Singa's CA*" as his Certification Authority.
- Add "*Singa's CA*" to his list of installed roots.
- Check "CRL" for "E-mail to Pete (Sam)" under Outgoing e-mail procedural settings.

iv) Right click on Pete's workstation and configure his e-mail application settings:

- Check “Authenticate e-mail”, “Authenticate Certificate” and “CRL” for “E-mail from Sam” under Incoming e-mail procedural settings.

b. Expected Results

If the player follows the procedures listed in the previous subsection, the scenario will complete Phase 1 and proceed to Phase 2 of the game. If the player executes any incorrect move, he/she may not be able to complete Phase 1. Table 4 summarizes the details of the tests in Test Case 2.

Table 4. Test Case 2 Expected results

Test ID	**Description**	**Expected Results**
2a	The player executes the game sequence as described in Section B2a. (Note: The order by which steps ii-v is to be performed does not matter.)	Pete will fulfill his objective to receive trusted e-mails from Sam.
2b	The player configures Pete’s workstation to authenticate Sam’s e-mail and certificate, but did not check the “CRL” option.	Pete will receive spoofed e-mails from Roy.
2c	The player configures Sam’s and Pete’s workstations to check the “CRL” option, but does not purchase the CRL server, i.e., does not perform steps i-ii.	Pete will not be able to receive e-mails from Sam and fail his user goal, as he needs to be able to connect to a CRL server to check the certificate revocation status.

c. Actual Results

Table 5 documents the actual results and checks if they meet the expected results.

Table 5. Test Case 2 Actual results

Test ID	Actual Results	Meets Expected Results?
2a	Pete achieved his goal and the game proceeded to Phase 2.	Yes
2b	Pete received spoofed e-mails from Roy. As a result, the player incurred monetary penalties.	Yes
2c	Pete could not receive e-mails from Sam. The game did not proceed to the next phase and shifted the screen display to Pete to notify the player that the user was not achieving his goal.	Yes

3. Test Case 3: Receiving of Dave's E-Mail

a. Scope of Test Case

Test Case 3 corresponds to the objective in Phase 2 of Cert Attack, which introduces the concept of certificate path processing. Dave will be tasked to send business specifications to Shirley, and the player has to perform the following procedures to enable Shirley to achieve this goal:

i) Right click on Shirley's workstation and configure her e-mail application settings:

- Check "Authenticate e-mail" and "Authenticate Certificate" for "E-mail from Dave" under Incoming e-mail procedural settings.

ii) Right click on *Pura's CA* and configure it to sign *Friendly CA.*

iii) When the quiz is launched at the end of Phase 2, click on the correct answer "D–Sign *Friendly's CA* (Dave's CA) certificate with *Pura's CA,* whose CA has been cross-certified with *Singa's CA*, which is a trusted root installed in Shirley's workstation.".

b. Expected Results

If the player follows the procedures listed in the previous subsection, the scenario will complete Phase 2 and proceed to Phase 3 of the game. If the player executes any incorrect move, he/she will need to attempt the quiz posted at the end of Phase 2 till he gets the correct answer before proceeding to Phase 3. Table 6 summarizes the details of the tests in Test Case 3.

Table 6. Test Case 3 Expected results

Test ID	**Description**	**Expected Results**
3a	The player executes the game sequence as described in Section B3a. (Note: The order by which steps i-ii is to be performed does not matter.)	Shirley will fulfill her objective to receive trusted e-mails from Dave.
3b	Instead of certifying *Friendly CA* via step ii, the player chooses to add *Friendly CA* to Shirley’s list of installed roots and may choose to submit the quiz response “B–Install *Friendly CA’s* (Dave’s CA) certificate as a trusted root in Shirley’s workstation.”	Shirley will be able to receive trusted e-mails from Dave, but the player will fail the objective because this deviates from the Singa’s policy, as stated in the scenario briefing and may answer the quiz incorrectly.
3c	The player chooses to sign *Friendly CA* by configuring *Singa’s CA* instead of *Pura’s CA* and may choose to submit the quiz response “C–*Sign Friendly CA’s* (Dave’s CA) certificate with *Singa’s CA*, which is already a trusted root installed in Shirley’s workstation.”	Shirley will be able to receive trusted e-mails from Dave, but the player may have misunderstood Singa’s policy, as stated in the scenario briefing and may answer the quiz incorrectly.

c. Actual Results

Table 7 documents the actual results and checks if they meet the expected results.

Table 7. Test Case 3 Actual results

Test ID	Actual Results	Meets Expected Results?
3a	Shirley achieved her goal. The player answered the quiz correctly and the game proceeded to Phase 3.	Yes
3b	The player answered the quiz incorrectly and had to resubmit the response till the right answer was obtained. The game then proceeded to Phase 3.	Yes
3c	The player answered the quiz incorrectly and had to resubmit the response till the right answer was obtained. The game then proceeded to Phase 3.	Yes

4. Test Case 4: Accessing of *Rival's* Web Page

a. Scope of Test Case

Test Case 4 corresponds to the objective in final phase of Cert Attack, which aims to illustrate the subtle, yet important difference between the digital signing key and the identity key. Shirley will be instructed to place a purchase order via *Rival's* webpage, which requires the player to set up TLS web client authentication by executing the following procedures:

i) Right click on Shirley's workstation and configure her web browser application settings:

- Select "*Singa's CA*" as her Certification Authority.
- When prompted to use existing certificate with Singa's CA, click "No".
- In the popup dialog box, click on "Get Certificate & Key Pair" to generate a new "Identity" certificate and select it.

b. Expected Results

If the player follows the procedures listed in the previous subsection, all the objectives of the game will be achieved and the player will win the game. If the player executes any incorrect move, he/she will observe an attack by Roy and will need to implement the appropriate countermeasure in order to complete the game. Table 8 summarizes the details of the tests in Test Case 4.

Table 8. Test Case 4 Expected results

Test ID	**Description**	**Expected Results**
4a	The player executes the game sequence as described in Section B4a.	Shirley will fulfill her objective to place orders securely on Rival’s webpage.
4b	The player fails to configure Shirley’s workstation’s browser settings to enable the TLS web client session.	Shirley will not be able to access *Rival’s* webpage and fail her user goal, as Rival’s web page requires TLS.
4c	The player chooses to use the existing e-mail certificate when he/she selects “*Singa’s CA*” as Shirley’s CA.	Shirley will be able to access *Rival’s* webpage to place her orders, but Roy will be able craft a spoofed e-mail to Pete by exploiting the challenge signed unknowingly by Shirley during the TLS web client authentication process.

c. Actual Results

Table 9 documents the actual results and checks if they meet the expected results.

Table 9. Test Case 4 Actual results

Test ID	**Actual Results**	**Meets Expected Results?**
4a	Shirley achieved her goal and the player completed the *Cert Attack* scenario.	Yes
4b	Shirley could not access *Rival's* webpage. The game did not complete and the screen display was shifted to Shirley to notify the player that the user was not achieving her goal.	Yes
4c	Roy was able to craft a spoofed e-mail to Pete by exploiting the challenge signed unknowingly by Shirley during the TLS web client authentication process and could use it to extort *Singa*. As a result, the player incurred monetary penalties.	Yes

C. SUMMARY

The test methodology and test cases developed for the Cert Attack scenario verified that it achieved its intended educational goals. The testing also validated that the feedback provided by the CyberCIEGE game engine was consistent with real-world implementations. Test logs generated for each of the test cases described above could also serve as input to regression testing as changes are introduced to the CyberCIEGE game engine in the future.

The next and final chapter concludes this thesis and proposes additional areas for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. CONCLUSION

This thesis focused on the current state of PKI implementations and understanding the pertinent variables that defined real-world PKI applications, which then led to the development of a CyberCIEGE scenario to depict the different configurations of PKI implementation and their corresponding security implications. By understanding the key concepts of PKI and subsequently researching on real-world implementation issues, suitable PKI functional elements were identified and modeled into the *Cert Attack* scenario. This new scenario is now an enhancement to the list of information security topic areas animated by CyberCIEGE.

Computer security is constantly evolving and it is essential for security practitioners and educators to remain current and be equipped with the necessary training tools to edify users on complex security policies and technologies. CyberCIEGE's interactive environment and extensible features allow *Cert Attack* to mimic real-world PKI issues and simulate feedback commensurate with real-world implementations. The lessons learnt from the development of this scenario can also be applied to the creation of new scenarios.

B. ADDITIONAL AREAS FOR FUTURE RESEARCH

There are a few areas that could be explored for future development. These areas are related to PKI security and interoperability issues, which could either be built upon the *Cert Attack* scenario or could form the storyboard for new scenarios. A few candidate examples follow.

1. Presentation of Bogus Certificates

In the *Cert Attack* scenario, when the player does not put in place the appropriate security measures to protect the e-mail assets, Roy will provide a description on how he was able to compromise the integrity of the e-mail. In particular, if the player allows the users to communicate using self-signed certificates, Roy will be able to create a "bogus certificate" to send spoofed e-mails. It would be useful to also present to the player a view of this "bogus certificate" to allow the player to compare how it differs from an actual certificate, and hence better appreciate the importance of making the correct security decision to protect the asset.

To facilitate this, a "View Certificate" button could be built in a popup message box after Roy describes the attack. When the attack occurs, Roy's bogus certificate would be automatically added into the certificate list in Shirley's workstation, such that Shirley would be able to select the bogus certificate and click on "View Certificate" button in the "Validate Cert" dialog box. It would also be recommended to update the date and time during which the bogus certificate was issued (i.e., when the attack occurred in the game), so that the player would be able to distinguish a certificate that is signed by the actual user and one that has been spoofed by Roy.

2. Modeling of CRL Semantics

The current version of the game engine is programmed to prompt the IT support staff to revoke any certificate that has been exposed via the *ExposeKey* trigger. Though this is sufficient for the introduction of the basic concept of certificate revocation for the learning objective prescribed in this thesis, the CyberCIEGE game engine could be further enhanced to present details on how full-scale certificate revocation mechanisms are implemented.

Future work could; for example, look into how the actual CRL structure (presented in Chapter II, Figure 4) can be modeled in CyberCIEGE to allow players to see/review the list of revoked certificates. The game engine can also be modified to update the status of the X.509 certificate interface to let the players observe the difference between normal certificates and revoked certificates.

Currently, the *Cert Attack* scenario is designed based on the assumption that all transactions are conducted online and that certificate revocation status are polled via a CRL distribution point. It would be useful to consider the case when the CRL distribution point is unreachable and the users may have to fall back to offline operations for some operational contingency. New CyberCIEGE scenarios could be developed to illustrate a different mode of online operation, i.e., the use of OCSP to provide more real-time and up-to-date certificate revocation and a representation on how organizations handle the contingent case when the OCSP service becomes unavailable. Coupled with the modeling of how e-mail clients or web browsers handle CRL checking, this would allow players to garner more in-depth PKI knowledge surrounding the important support infrastructure issue of certificate revocation.

3. Web Client Authentication Educational Video

The final phase of the current *Cert Attack* scenario scales the requirement from e-mail communications to also include Web access. Currently, Roy will provide a verbal description on how he exploits the misconfigured Web client authentication settings. It would be beneficial if the player could see a video sequence of the Web client authentication procedures and how the individual steps could be exploited using a myriad of attacks (e.g., replay, man-in-the-middle, etc.).

4. Testing with Students

The test cases presented in Chapter V were derived based on anticipated player actions. It would be more fruitful to involve the intended audience in the testing phase to verify that the game does provide the necessary feedback to facilitate autonomous game play, and that the players actually do comprehend and learn the targeted PKI learning objectives. This scenario could be provided to NPS students in the Information Operations & Assurance track, whose game/scenario play could provide valuable feedback to further improve the scenario.

LIST OF REFERENCES

22nd Open Grid Forum. (2008, February 28). Private key protection. Cambridge, MA.

Adams, C., & Lloyd, S. (2003). *Understanding PKI: Concepts, standards and deployment considerations.* Upper Saddle River, NJ: Pearson Education, Inc.

Allen, K., Irvine, C., & Thompson, M. (2005, June). CyberCIEGE: An Extensible Tool for Information Assurance Education. *9th Colloquium for Information Systems*. Atlanta, GA.

Blackbaud, Inc. (2006, March). *Effective e-mail communications.* Retrieved from http://www.blackbaud.com/files/resources/downloads/WhitePaper_EffectiveE-mailCommunications.pdf

Bright, P. (2011, September). *Comodo hacker: I hacked DigiNotar too; other CAs breached.* Retrieved from ars technica: http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars

CyberCIEGE Scenario development tool user's guide. (2011, September). Monterey, CA: The Center for Information Systems Security Studies and Research.

Federal PKI Policy Authority. (2007, January 29). *Registration authority (RA) requirements.* Retrieved October 21, 2011, from IDManagement.GOV: http://www.idmanagement.gov/fpkipa/documents/RArequirements.pdf

Fulp, J. (2011). *Teaching in Network Security*. Monterey, CA: Naval Postgraduate School.

Hofman, M. (2011, September 10). *The impact of Diginotar on certificate authorities and trust.* Retrieved from Internet Storm Center: http://isc.sans.edu/diary.html?storyid=11560

Housley, R., Polk, W., Ford, W., & Solo, D. (2002, Apr). *Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile.* Retrieved from Network Working Group RFC 3280: http://www.ietf.org/rfc/rfc3280.txt

Identity, Credential and Access Management Sub Committee (ICAMSC). (2010). *The realized value of the federal public key infrastructure (FPKI).* Washington, DC: ICAMSC

Irvine, C., & Thompson, M. (2010, November 1–3). Simulation of PKI-enabled communication for identity management using CyberCIEGE. *Military Communications Conference*, San Jose, CA.

Irvine, C., & Thompson, M. (2003, June 24–27). Teaching Objectives of a Simulation Game for Computer Security. *Informing Science and Information Technology Joint Conference*, Pori, Finland.

Public key infrastructure. (2011, October 11). In *Wikipedia*. Retrieved October 20, 2011, from http://en.wikipedia.org/wiki/Public_key_infrastructure

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. George Bieber
   Office of the Secretary of Defense
   Washington, DC

4. Sue Fitgerald
   National Science Foundation
   Arlington, Virginia

5. Peggy Maxson
   Department of Homeland Security
   Washington, DC

6. Victor Piotrowski
   National Science Foundation
   Arlington, Virginia

7. Dr. Cynthia E. Irvine
   Naval Postgraduate School
   Monterey, California

8. J.D. Fulp
   Naval Postgraduate School
   Monterey, California

9. Mike Thompson
   Naval Postgraduate School
   Monterey, California

10. Prof. Yeo Tat Soon
    Director of Temasek Defence System Institute
    National University of Singapore
    Singapore

11. Tan Lai Poh
National University of Singapore
Singapore

12. Ng Teng Teng
Student, Naval Postgraduate School
Monterey, California